ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Πρόγραμμα Μεταπτυχιακών Σπουδών

«ΔΙΚΑΙΟ ΚΑΙ ΤΕΧΝΟΛΟΓΙΕΣ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ»

Ακαδημαϊκό έτος 2024-2025

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ
ΠΑΝΑΓΙΩΤΗ Ε. ΑΝΔΡΕΟΥ (ΜΔΙ 2304)

ΕΥΡΩΠΑΪΚΗ ΟΔΗΓΙΑ 2022/2555 (NIS 2): ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ ΚΑΙ ΠΡΑΚΤΙΚΟ ΠΛΑΙΣΙΟ ΕΛΕΓΧΟΥ ΣΥΜΜΟΡΦΩΣΗΣ ΜΕ ΤΗΝ NIS2 ΚΑΙ ΤΟΝ ΕΦΑΡΜΟΣΤΙΚΟ ΝΟΜΟ 5160/2024

[EUROPEAN DIRECTIVE 2022/2555 (NIS 2): CYBERSECURITY AND A PRACTICAL COMPLIANCE AUDIT FRAMEWORK FOR NIS2 AND THE IMPLEMENTING LAW 5160/2024]

Επιβλέπων:

Καθηγητής Στέφανος Γκρίτζαλης

Πειραιάς, Ιανουάριος 2026

Η σελίδα αυτή είναι σκόπιμα κενή

ΠΕΡΙΕΧΟΜΕΝΑ

ΠΡΟΛΟΓΟΣ

Με την ολοκλήρωση της παρούσας διπλωματικής μου θα ήθελα να εκφράσω τις θερμές μου ευχαριστίες προς τον επιβλέποντα καθηγητή μου, κ. Στέφανο Γκρίτζαλη για την καθοδήγηση, τη στήριξη και τις πολύτιμες επιστημονικές του παρατηρήσεις καθ' όλη την διάρκεια εκπόνησης της παρούσας διπλωματικής εργασίας.

Ευχαριστώ επίσης την οικογένειά μου για την αμέριστη ηθική υποστήριξη και κατανόηση, καθώς και όλους όσους συνέβαλαν με τον τρόπο τους στην ολοκλήρωση αυτής της προσπάθειας.

ΠΕΡΙΛΗΨΗ

Η ραγδαία εξέλιξη των τεχνολογιών πληροφορικής και επικοινωνιών, σε συνδυασμό με τη συνεχή ψηφιοποίηση των οικονομικών, κοινωνικών και διοικητικών δραστηριοτήτων, έχει μετασχηματίσει ριζικά τον τρόπο λειτουργίας των επιχειρήσεων και των οργανισμών. Η αυξανόμενη εξάρτηση από ψηφιακές υποδομές, πληροφοριακά συστήματα και δικτυακές υπηρεσίες έχει αναδείξει την κυβερνοασφάλεια σε κρίσιμο παράγοντα για τη διασφάλιση της επιχειρησιακής συνέχειας, της προστασίας των δεδομένων και της εύρυθμης λειτουργίας τόσο του ιδιωτικού όσο και του δημόσιου τομέα. Παράλληλα, η ίδια αυτή ψηφιακή εξάρτηση έχει διευρύνει σημαντικά την επιφάνεια επίθεσης, καθιστώντας τα πληροφοριακά συστήματα ευάλωτα σε ολοένα και πιο σύνθετες και εξελιγμένες κυβερνοαπειλές.

Το κυβερνοέγκλημα, οι κυβερνοεπιθέσεις και οι οργανωμένες κακόβουλες δραστηριότητες στον κυβερνοχώρο αποτελούν πλέον συστημικούς κινδύνους, με σοβαρές οικονομικές, κοινωνικές και θεσμικές επιπτώσεις. Επιθέσεις όπως το ηλεκτρονικό ψάρεμα (phishing), το κακόβουλο λογισμικό (malware), το λυτρισμικό (ransomware) και οι επιθέσεις άρνησης παροχής υπηρεσιών (DDoS) δεν πλήττουν μόνο την τεχνική υποδομή των οργανισμών, αλλά επηρεάζουν άμεσα την εμπιστοσύνη των χρηστών, την προστασία των προσωπικών δεδομένων και, σε ορισμένες περιπτώσεις, την εθνική ασφάλεια. Στο περιβάλλον αυτό, η κυβερνοασφάλεια δεν αποτελεί πλέον αποκλειστικά τεχνικό ζήτημα, αλλά εντάσσεται στον πυρήνα της οργανωτικής διακυβέρνησης, της κανονιστικής συμμόρφωσης και της νομικής ευθύνης των επιχειρήσεων και των οργανισμών.

Σε ευρωπαϊκό επίπεδο, η ανάγκη για ένα ενιαίο, συνεκτικό και αποτελεσματικό κανονιστικό πλαίσιο οδήγησε στην υιοθέτηση της Οδηγίας (ΕΕ) 2022/2555, γνωστής ως Οδηγίας NIS2, η οποία αντικατέστησε και ενίσχυσε το προϋφιστάμενο πλαίσιο της Οδηγίας NIS1. Η NIS2 εισάγει αυστηρότερες και σαφέστερες υποχρεώσεις για ένα ευρύτερο φάσμα επιχειρήσεων και οργανισμών, χαρακτηρίζοντάς τους ως βασικές και σημαντικές οντότητες, και καθιερώνει ένα σύστημα διαχείρισης κινδύνων κυβερνοασφάλειας βασισμένο στην αρχή της αναλογικότητας και της λογοδοσίας. Κεντρικός άξονας της Οδηγίας αποτελεί η υποχρέωση υιοθέτησης κατάλληλων

τεχνικών, οργανωτικών και επιχειρησιακών μέτρων, καθώς και η έγκαιρη αναφορά και διαχείριση περιστατικών κυβερνοασφάλειας.

Η Ελλάδα ενσωμάτωσε την Οδηγία NIS2 στο εθνικό δίκαιο με τον Νόμο 5160/2024, ο οποίος συνιστά το νέο θεσμικό πλαίσιο για την κυβερνοασφάλεια στη χώρα. Ο νόμος αυτός εκσυγχρονίζει τις διατάξεις του προηγούμενου Ν. 4577/2018 και θεμελιώνει ένα ολοκληρωμένο σύστημα διακυβέρνησης της κυβερνοασφάλειας, καθορίζοντας αρμόδιες αρχές, μηχανισμούς εποπτείας και ελέγχου, καθώς και κυρώσεις για τη μη συμμόρφωση των υπόχρεων οντοτήτων. Παράλληλα, μέσω κανονιστικών πράξεων και ειδικότερα της Υπουργικής Απόφασης 1689/2025, εξειδικεύονται οι απαιτήσεις συμμόρφωσης και προσδιορίζονται συγκεκριμένες πολιτικές, διαδικασίες και μέτρα ασφάλειας που οφείλουν να εφαρμόζουν οι βασικές και σημαντικές οντότητες.

Σκοπός της παρούσας διπλωματικής εργασίας είναι η συστηματική ανάλυση του κανονιστικού και οργανωτικού πλαισίου κυβερνοασφάλειας που εισάγει η Οδηγία NIS2 και ο εφαρμοστικός Νόμος 5160/2024, καθώς και η παρουσίαση ενός πρακτικού πλαισίου ελέγχου συμμόρφωσης για επιχειρήσεις και οργανισμούς. Η εργασία επιδιώκει να γεφυρώσει τη θεωρητική προσέγγιση της κυβερνοασφάλειας με την πρακτική εφαρμογή των κανονιστικών απαιτήσεων, αναδεικνύοντας τον ρόλο των οργανωτικών προτύπων, των τεχνικών μέτρων και των θεσμικών μηχανισμών επιβολής.

Η μεθοδολογία που ακολουθείται βασίζεται στη συνδυαστική ανάλυση τεχνικών, οργανωτικών και νομικών πηγών, συμπεριλαμβανομένων ευρωπαϊκών οδηγιών, εθνικών νομοθετημάτων, διεθνών προτύπων ασφάλειας πληροφοριών και κανονιστικών πράξεων. Ιδιαίτερη έμφαση δίνεται στη διαχείριση κινδύνων κυβερνοασφάλειας, στον ρόλο των αρμόδιων αρχών, στις υποχρεώσεις αναφοράς περιστατικών και στη σημασία της επιχειρησιακής συνέχειας και της διαχείρισης κρίσεων.

Η δομή της εργασίας αντανακλά τη σταδιακή ανάπτυξη του αντικειμένου. Αρχικά, παρουσιάζονται βασικές έννοιες που σχετίζονται με την κυβερνοασφάλεια, το κυβερνοέγκλημα και τις τεχνολογικές εξελίξεις. Στη συνέχεια, αναλύονται οι μορφές και οι τύποι κυβερνοεπιθέσεων και οι επιπτώσεις τους στις επιχειρήσεις και στους οργανισμούς. Ακολουθεί η εξέταση των οργανωτικών προτύπων ασφάλειας πληροφοριών και του κανονιστικού πλαισίου κυβερνοασφάλειας, τόσο σε ευρωπαϊκό όσο και σε εθνικό επίπεδο. Ιδιαίτερη ενότητα αφιερώνεται στις αρμόδιες αρχές επιβολής της

νομοθεσίας, καθώς και στον ρόλο του Υπεύθυνου Ασφάλειας Συστημάτων Πληροφορικής και Επικοινωνιών (Υ.Α.Σ.Π.Ε.). Τέλος, αναλύονται διεξοδικά τα τεχνικά και οργανωτικά μέτρα ασφάλειας, οι υποχρεώσεις αναφοράς περιστατικών και οι μηχανισμοί επιχειρησιακής συνέχειας, στο πλαίσιο της συμμόρφωσης με τη NIS2.

Μέσα από αυτή τη συστηματική προσέγγιση, η παρούσα εργασία φιλοδοξεί να συμβάλει στην κατανόηση της κυβερνοασφάλειας ως πολυδιάστατου πεδίου, όπου η τεχνολογία, η οργάνωση και το δίκαιο αλληλεπιδρούν, και να προσφέρει ένα πρακτικό εργαλείο αναφοράς για την εφαρμογή και τον έλεγχο συμμόρφωσης με το σύγχρονο ευρωπαϊκό και εθνικό πλαίσιο κυβερνοασφάλειας.

ABSTRACT

The rapid development of information and communication technologies, combined with the continuous digitalisation of economic, social, and administrative activities, has fundamentally transformed the way businesses and organisations operate. The increasing reliance on digital infrastructures, information systems, and network services has elevated cybersecurity to a critical factor for ensuring business continuity, data protection, and the proper functioning of both the private and public sectors. At the same time, this growing dependence on digital systems has significantly expanded the attack surface, rendering information systems more vulnerable to increasingly sophisticated and evolving cyber threats.

Cybercrime, cyberattacks, and organised malicious activities in cyberspace now constitute systemic risks with serious economic, social, and institutional consequences. Attacks such as phishing, malware infections, ransomware incidents, and distributed denial-of-service (DDoS) attacks not only compromise the technical integrity of information systems but also directly affect user trust, the protection of personal data, and, in certain cases, national security. In this context, cybersecurity can no longer be regarded as a purely technical issue; rather, it has become a core element of organisational governance, regulatory compliance, and legal accountability for businesses and organisations.

At the European level, the need for a unified, coherent, and effective regulatory framework led to the adoption of Directive (EU) 2022/2555, commonly referred to as the NIS2 Directive, which repealed and substantially reinforced the previous NIS1 framework. NIS2 introduces stricter and more clearly defined obligations for a broader range of entities, categorising them as essential and important entities, and establishes a risk-based approach to cybersecurity governance grounded in the principles of proportionality and accountability. A central pillar of the Directive is the obligation to implement appropriate technical, organisational, and operational cybersecurity risk management measures, as well as to ensure timely incident reporting and response.

Greece transposed the NIS2 Directive into national law through Law 5160/2024, which constitutes the new institutional framework for cybersecurity in the country. This law modernises the provisions of the former Law 4577/2018 and establishes an integrated

cybersecurity governance system, defining competent authorities, supervisory and enforcement mechanisms, and sanctions for non-compliance by obligated entities. Furthermore, through secondary legislation—most notably Ministerial Decision No. 1689/2025—the general obligations introduced by NIS2 and Law 5160/2024 are further specified by defining concrete cybersecurity policies, procedures, and security measures that essential and important entities are required to adopt and implement.

The purpose of this thesis is to provide a systematic analysis of the regulatory and organisational cybersecurity framework introduced by the NIS2 Directive and its implementing Law 5160/2024, as well as to present a practical compliance audit framework applicable to businesses and organisations. The thesis aims to bridge the gap between the theoretical foundations of cybersecurity and the practical implementation of regulatory requirements, highlighting the role of organisational standards, technical safeguards, and institutional enforcement mechanisms.

The methodology adopted in this study is based on a combined analysis of technical, organisational, and legal sources, including European directives, national legislation, international information security standards, and regulatory acts. Particular emphasis is placed on cybersecurity risk management, the role of competent authorities, incident reporting obligations, and the importance of business continuity and crisis management mechanisms.

The structure of the thesis reflects the progressive development of the subject matter. Initially, fundamental concepts related to cybersecurity, cybercrime, and technological evolution are presented. Subsequently, the main forms and types of cyberattacks and their impact on businesses and organisations are analysed. The thesis then examines organisational information security standards and the cybersecurity regulatory framework at both European and national levels. A dedicated chapter focuses on the competent authorities responsible for the enforcement of cybersecurity legislation, as well as on the role of the Information and Communication Systems Security Officer (ICSSO). Finally, the thesis provides an in-depth analysis of technical and organisational security measures, incident reporting obligations, and business continuity and crisis management mechanisms within the framework of compliance with NIS2.

Through this comprehensive approach, the present thesis seeks to contribute to the understanding of cybersecurity as a multidimensional field in which technology, organisational governance, and law interact, while also offering a practical reference tool for the implementation and compliance assessment of the contemporary European and national cybersecurity framework.

1. ΕΙΣΑΓΩΓΗ ΣΤΗΝ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ

1.1 Κυβερνοέγκλημα, κυβερνοασφάλεια και τεχνολογικές αλλαγές

Η τεχνολογία των υπολογιστών έχει εξελιχθεί σε μεγάλο βαθμό όσον αφορά την πολυπλοκότητα και την καινοτομία με το πέρασμα των χρόνων. Η πλειοψηφία αυτών των εξελίξεων, μαζί με τη δύναμη και την εμβέλεια του Διαδικτύου, έχει ενισχύσει τη δημοτικότητα της τεχνολογίας των πληροφοριών, καθιστώντας τη σχεδόν απαραίτητη σε κάθε τομέα ή σε κάθε άτομο που χρησιμοποιεί συστήματα και δίκτυα υπολογιστών για επαγγελματικούς, εκπαιδευτικούς ή άλλους σκοπούς.

Ιδιαίτερα, το διαδίκτυο έχει αναδειχθεί σε έναν πλούσιο πόρο γνώσης, ο οποίος είναι εύκολα προσβάσιμος από όλους, συνεπώς και από εγκληματίες του κυβερνοχώρου. Ωστόσο οι τελευταίοι, εν αντιθέσει με τους καλόπιστους χρήστες του διαδικτύου, αξιοποιώντας την παρεχόμενη πληροφορία και τις σύγχρονες τεχνολογίες, αναπτύσσουν προηγμένα εργαλεία και μεθόδους για τη διενέργεια κακόβουλων δραστηριοτήτων, μέσω των οποίων, είτε αλλοιώνουν την ακεραιότητα είτε υποκλέπτουν την εμπιστευτικότητα ευαίσθητων προσωπικών δεδομένων και πληροφοριών από επιχειρήσεις και οργανισμούς, με σκοπό την αποκόμιση παράνομου οικονομικού οφέλους. Βεβαίως, οι ενέργειές τους αυτές προκαλούν εμπόδια στην καινοτομία, στην ανταλλαγή γνώσεων, στην οικονομική ανάπτυξη καθώς και την ελεύθερη ροή των πληροφοριών, υπονομεύοντας εν τέλει την ίδια την αξία του ψηφιακού περιβάλλοντος και τον θεμελιώδη σκοπό υιοθέτησής του, δηλαδή την οικοδόμηση μιας ανοιχτής και ασφαλούς Κοινωνίας της Πληροφορίας.

1.1.1 Το έγκλημα στον Κυβερνοχώρο (Cybercrime)

Το κυβερνοέγκλημα συνιστά μια διαρκώς κλιμακούμενη απειλή με σοβαρές προεκτάσεις στην παγκόσμια ασφάλεια και οικονομία. Οι επιθέσεις στον ψηφιακό χώρο χαρακτηρίζονται πλέον από υψηλή συχνότητα, στοχοποίηση και τεχνολογική πολυπλοκότητα, θέτοντας σε άμεσο κίνδυνο υποδομές ζωτικής σημασίας, όπως οι δημόσιες υπηρεσίες, τα εθνικά αμυντικά δίκτυα και τα συστήματα ελέγχου της εναέριας κυκλοφορίας. Οι φορείς των επιθέσεων αυτών επιδιώκουν συστηματικά την απόσπαση

εμπορικών απορρήτων και ευαίσθητων δεδομένων, πλήττοντας τη στρατηγική λειτουργία επιχειρήσεων και οργανισμών, ενώ παράλληλα το φαινόμενο επεκτείνεται στην οικονομική εξαπάτηση ιδιωτών και την εκμετάλλευση ανηλίκων.

Υπό το πρίσμα αυτής της έξαρσης και των συνεχών παραβιάσεων, καθίσταται επιτακτική η υιοθέτηση στιβαρών στρατηγικών κυβερνοασφάλειας. Η θωράκιση των πληροφοριακών συστημάτων αποτελεί πλέον προϋπόθεση για τη διασφάλιση της ακεραιότητας, της εμπιστευτικότητας και της διαθεσιμότητας των δεδομένων, διαφυλάσσοντας ταυτόχρονα την αξιοπιστία των ψηφιακών συναλλαγών στο σύγχρονο επιχειρηματικό περιβάλλον.

1.1.2 Κυβερνοεπίθεση (Cyber Attack)

Η κυβερνοεπίθεση ως ενέργεια ορίζεται η εσκεμμένη και κακόβουλη απόπειρα παραβίασης ενός ψηφιακού συστήματος από μεμονωμένα άτομα ή οργανωμένες ομάδες, με αντικειμενικό σκοπό την υποκλοπή, την αλλοίωση ή την καταστροφή δεδομένων. Μολονότι τα κίνητρα ποικίλλουν, στον πυρήνα των δραστηριοτήτων αυτών βρίσκεται η επιδίωξη αποκόμισης παράνομου περιουσιακού οφέλους, η πρόκληση λειτουργικής ζημίας ή η απόκτηση στρατηγικού πλεονεκτήματος έναντι αντιπάλων. Οι επιθέσεις αυτές συνιστούν θεμελιώδη απειλή για την ασφάλεια των πληροφοριών, καθώς στοχεύουν στην παραβίαση της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των δεδομένων (CIA Triad), πλήττοντας συχνά υποδομές ζωτικής σημασίας.

Το πεδίο στοχοποίησης των κυβερνοεγκλημάτων περιλαμβάνει κρίσιμες δικτυακές συνιστώσες, με έμφαση στους διακομιστές (servers) που υποστηρίζουν τη λειτουργία οργανισμών και κυβερνητικών φορέων. Ειδικότερα, στοχεύονται διακομιστές δεδομένων (data servers) για την απόσπαση βάσεων δεδομένων που περιέχουν εμπιστευτικές πληροφορίες, διακομιστές εφαρμογών (application servers) για τη διακοπή κρίσιμων λειτουργιών, καθώς και διακομιστές αποθήκευσης (storage servers) λόγω του μεγάλου όγκου ευαίσθητων αρχείων που φιλοξενούν. Παράλληλα, ιδιαίτερη βαρύτητα δίνεται στις οικονομικές πληροφορίες (financial information), όπου η υποκλοπή

τραπεζικών δεδομένων και στοιχείων συναλλαγών διευκολύνει την οικονομική απάτη, τον εκβιασμό ή τη βιομηχανική κατασκοπεία.

Η εκτέλεση των κυβερνοεπθέσεων βασίζεται σε μια διαρκώς εξελισσόμενη εργαλειοθήκη τεχνικών. Μεταξύ αυτών δεσπόζει η χρήση κακόβουλου λογισμικού (malware), όπως οι ιοί και το ransomware, η κοινωνική μηχανική μέσω του ηλεκτρονικού ψαρέματος (phishing) για την απόσπαση διαπιστευτηρίων, καθώς και η εκμετάλλευση τρωτών σημείων μέσω εισαγωγής κακόβουλου κώδικα (SQL Injection) για τη μη εξουσιοδοτημένη πρόσβαση σε βάσεις δεδομένων. Επιπλέον, οι επιθέσεις άρνησης υπηρεσίας (DoS/DDoS) αποσκοπούν στην κατάλυση της διαθεσιμότητας ενός συστήματος μέσω του τεχνητού κορεσμού των πόρων του, ενώ η μέθοδος της ενδιάμεσης παρεμβολής (Man-in-the-Middle) επιτρέπει την κρυφή υποκλοπή ή τροποποίηση της επικοινωνίας μεταξύ δύο μερών σε πραγματικό χρόνο.

Η πολυμορφία και η συνεχής τεχνολογική αναβάθμιση αυτών των μεθόδων — που εκτείνονται από την εταιρική δυσφήμιση έως την κυβερνοτρομοκρατία— καθιστούν αναγκαία την υιοθέτηση μιας ολιστικής στρατηγικής άμυνας. Αυτή περιλαμβάνει την εφαρμογή προηγμένων συστημάτων ανίχνευσης, τη διαρκή εκπαίδευση του ανθρώπινου δυναμικού και την αυστηρή τήρηση των διεθνών προτύπων κυβερνοασφάλειας, ώστε να διασφαλιστεί η σταθερότητα του ψηφιακού οικοσυστήματος.

1.1.3 **Κυβερνοασφάλεια (Cybersecurity)**

Η κυβερνοασφάλεια (Cybersecurity) αναφέρεται στο σύνολο των βασικών πρακτικών που αποσκοπούν στην προστασία του λογισμικού, του υλικού και των δεδομένων που είναι συνδεδεμένα στο διαδίκτυο ή αποθηκευμένα σε αυτό. Περιλαμβάνει την αλληλεπίδραση μεταξύ ανθρώπων, τεχνολογίας και διαδικασιών, είτε σε έναν οργανισμό, είτε σε μια ομάδα, είτε σε ένα μεμονωμένο περιβάλλον. Ο τομέας αυτός αποτελεί έναν από τους σημαντικότερους κλάδους της τεχνολογίας πληροφοριών, καθώς επηρεάζει τόσο τους ιδιώτες, όσο και τις επιχειρήσεις κάθε μεγέθους. Η ραγδαία ανάπτυξη της κυβερνοασφάλειας οφείλεται στην αυξανόμενη χρήση και εξάρτηση από το διαδίκτυο, τους υπολογιστές και τα ασύρματα δίκτυα. Είναι γεγονός πως η διάδοση έξυπνων συσκευών, όπως είναι τα smartphones, οι smart TVs και οι συσκευές που

ανήκουν στο «Διαδίκτυο των Πραγμάτων» (IoT), έχει αυξήσει την ανάγκη για αποτελεσματικότερα μέτρα ασφαλείας. Οι πολιτικές και οι τεχνολογίες που ρυθμίζουν τη χρήση του διαδικτύου και των ψηφιακών συστημάτων είναι εξαιρετικά περίπλοκες, καθώς ενσωματώνουν τεχνικά ζητήματα και απαιτούν προηγμένα εξειδικευμένα εργαλεία.

Μια αποτελεσματική στρατηγική προσέγγιση για την κυβερνοασφάλεια είναι η υιοθέτηση του μοντέλου **Zero Trust** που βασίζεται στην αρχή "**ποτέ μην εμπιστεύεσαι, πάντα επαλήθευσε**". Στόχος της εν λόγω στρατηγικής είναι η συνεχής επαλήθευση χρηστών και συσκευών, η ελαχιστοποίηση των κινδύνων και η βελτίωση της προστασίας έναντι επιθέσεων. Η εφαρμογή του συγκεκριμένου μοντέλου απαιτεί πολυεπίπεδη προσέγγιση, η οποία περιλαμβάνει την ανάλυση και την αξιολόγηση τυχόν κινδύνων, την εφαρμογή της αρχής της ελάχιστης πρόσβασης (Least Privilege Access), την ενίσχυση του ελέγχου ταυτότητας χρηστών και συσκευών, την μικροτμηματοποίηση του υφιστάμενου δικτύου (Microsegmentation) καθώς επίσης και την συνεχή επιτήρηση και απόκριση σε εισερχόμενες απειλές.

Όπως καθίσταται αντιληπτό, ο τομέας της κυβερνοασφάλειας είναι δυναμικός και περιλαμβάνει διαφορετικές τεχνολογίες για την αντιμετώπιση της ποικιλομορφίας των κυβερνοεπιθέσεων. Έτσι, παρόλο που δεν υπάρχει αυστηρά καθορισμένη ταξινόμηση, μια ενδεικτική κατηγοριοποίηση περιλαμβάνει:

- Ασφάλεια δικτύων (Network Security - NS) : Προστασία δικτύων από εισβολές και κακόβουλες ενέργειες.
- Ασφάλεια Πληροφοριών (Information Security – IS): Διασφάλιση της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας δεδομένων.
- Ασφάλεια εφαρμογών (Application Security – AS): Προστασία λογισμικού από ευπαθείς επιθέσεις.
- Σχεδιασμός επιχειρησιακής συνέχειας και αποκατάστασης πληροφοριών (Business Continuity Planning -BCP & Disaster Recovery): Στρατηγικές για την αντιμετώπιση κρίσεων και την αποκατάσταση λειτουργιών μετά από κυβερνοεπιθέσεις.
- Δέσμευση ηγεσίας (Leadership): Εξασφάλιση της υποστήριξης από τη διοίκηση για την εφαρμογή πολιτικών ασφαλείας.

- Επιχειρησιακή ασφάλεια (Operation Security – OPSSEC): Εξέταση κινδύνων που αφορούν τη διαχείριση δεδομένων και πληροφοριών.
- Εκπαίδευση τελικών χρηστών (End – User Education): Ευαισθητοποίηση και εκπαίδευση των χρηστών, έτσι ώστε να αναγνωρίζουν και να αποφεύγουν απειλές.

1.1.4 Πλεονεκτήματα – Μειονεκτήματα Κυβερνοασφάλειας

Η εφαρμογή μέτρων κυβερνοασφάλειας είναι ζωτικής σημασίας για την προστασία των πληροφοριακών συστημάτων, των δεδομένων και της ιδιωτικότητας. Στο πλαίσιο αυτό, η κυβερνοασφάλεια δεν παρουσιάζει μόνο σημαντικά πλεονεκτήματα, αλλά και ορισμένα μειονεκτήματα, τα οποία σχετίζονται κυρίως με τις απαιτήσεις συμμόρφωσης, την διαθεσιμότητα πόρων καθώς και την ανάγκη συνεχούς προσαρμογής στις εξελισσόμενες απειλές.

Ειδικότερα, τα πλεονεκτήματα της κυβερνοασφάλειας είναι πολλαπλά. Καταρχάς, διασφαλίζεται η προστασία των υπολογιστικών συστημάτων από κακόβουλες επιθέσεις, όπως επιθέσεις malware, ransomware, DDoS και phishing, οι οποίες μπορούν να προκαλέσουν σοβαρές ζημίες τόσο σε ατομικό όσο και σε επιχειρησιακό επίπεδο. Παράλληλα, αποτρέπεται η μη εξουσιοδοτημένη πρόσβαση σε δεδομένα και εφαρμογές, διασφαλίζοντας ότι μόνο εξουσιοδοτημένοι χρήστες διαθέτουν δικαίωμα πρόσβασης σε κρίσιμες πληροφορίες. Επιπλέον, η δυνατότητα αποκλεισμού πρόσβασης σε μολυσμένους πόρους μειώνει τον κίνδυνο εξάπλωσης κακόβουλου λογισμικού εντός ενός δικτύου και, κατ' επέκταση, την πιθανότητα εκτεταμένων παραβιάσεων ασφάλειας. Τέλος, η κυβερνοασφάλεια ενισχύει την εμπιστευτικότητα και την ακεραιότητα των δεδομένων, συμβάλλοντας στη διατήρηση της εμπιστοσύνης πελατών και συνεργατών, στοιχείο ιδιαίτερα κρίσιμο για επιχειρήσεις και οργανισμούς που διαχειρίζονται ευαίσθητες πληροφορίες.

Ωστόσο, η εφαρμογή ισχυρών μέτρων κυβερνοασφάλειας συνοδεύεται και από μειονεκτήματα που δεν μπορούν να αγνοηθούν. Ένα από τα βασικότερα προβλήματα είναι οι αυστηροί κανονισμοί και οι απαιτήσεις συμμόρφωσης, οι οποίοι συχνά απαιτούν σημαντικούς πόρους και εξειδικευμένη γνώση για την πλήρη εφαρμογή τους. Η

συμμόρφωση με νομοθετικά πλαίσια, όπως ο Γενικός Κανονισμός για την Προστασία Δεδομένων (General Data Protection Regulation - GDPR) ή η Οδηγία για την Κυβερνοασφάλεια NIS2, συνεπάγεται αυξημένες υποχρεώσεις για τις επιχειρήσεις, οι οποίες ενδέχεται να δυσκολευτούν να ανταποκριθούν στις απαιτήσεις αυτές. Επιπλέον, η κατανόηση και η εφαρμογή των μέτρων κυβερνοασφάλειας μπορεί να είναι ιδιαίτερα δύσκολη για μη τεχνικούς χρήστες, γεγονός που αυξάνει την ανάγκη για συνεχή εκπαίδευση και ευαισθητοποίηση.

Ένα άλλο σημαντικό μειονέκτημα είναι οι περιορισμένοι πόροι, ιδιαίτερα σε μικρότερους οργανισμούς που δεν διαθέτουν εξειδικευμένο προσωπικό ή επαρκή χρηματοδότηση για την επένδυση σε σύγχρονες λύσεις κυβερνοασφάλειας. Επιπλέον, οι οργανισμοί καλούνται να αντιμετωπίσουν τη συνεχή ανάγκη για αναβαθμίσεις και επιδιορθώσεις, καθώς οι κυβερνοαπειλές εξελίσσονται διαρκώς και οι υπάρχουσες λύσεις γίνονται αναποτελεσματικές απέναντι σε νέες επιθέσεις.

Τέλος, η κυβερνοασφάλεια δεν αποτελεί μια στατική κατάσταση, αλλά μια διαρκή πρόκληση, καθώς οι επιχειρήσεις και οι οργανισμοί είναι συνεχώς εκτεθειμένοι σε νέες απειλές και εξελιγμένες κυβερνοεπιθέσεις, οι οποίες απαιτούν συνεχή επαγρύπνηση και προσαρμογή των αμυντικών τους μηχανισμών.

1.1.5 Τεχνολογικές αλλαγές και Κυβερνοασφάλεια

Η κυβερνοασφάλεια βρίσκεται σε συνεχή εξέλιξη, καθώς οι απειλές που αναδύονται στον ψηφιακό χώρο καθίστανται ολοένα και πιο σύνθετες. Παρότι ο βασικός της στόχος παραμένει η προστασία των ψηφιακών συστημάτων και των πληροφοριών, οι μέθοδοι και τα μέσα που χρησιμοποιούνται μεταβάλλονται σημαντικά με την πάροδο του χρόνου. Τεχνολογίες που στο παρελθόν θεωρούνταν επαρκείς για την αντιμετώπιση κινδύνων σήμερα χαρακτηρίζονται ξεπερασμένες, λόγω των ραγδαίων τεχνολογικών εξελίξεων και της εμφάνισης νέων μορφών κυβερνοεπιθέσεων. Στο πλαίσιο αυτό, η ταχεία ανάπτυξη του διαδικτύου, των υπολογιστικών συστημάτων και των έξυπνων συσκευών έχει καταστήσει την ανάγκη για καινοτόμες λύσεις προστασίας ιδιαιτέρως επιτακτική.

Οι τεχνολογικές εξελίξεις επηρεάζουν άμεσα την ασφάλεια στον κυβερνοχώρο, στο μέτρο που οι σύγχρονες καινοτομίες και οι βελτιώσεις στην καθημερινή ζωή βασίζονται ολοένα και περισσότερο στη χρήση ψηφιακών συστημάτων και δικτυακών υποδομών. Καθώς η τεχνολογική πρόοδος επιταχύνεται, αυξάνεται αντίστοιχα και η συχνότητα των κυβερνοεπιθέσεων, γεγονός που μεταβάλλει ριζικά το περιβάλλον κινδύνων. Ενδεικτικά, στο παρελθόν η προστασία δεδομένων σε ένα επιχειρηματικό περιβάλλον περιοριζόταν, κατά κανόνα, στην αποθήκευση αρχείων σε φυσικά μέσα, όπως μεταλλικούς φοριαμούς, οι οποίοι ήταν προσβάσιμοι μόνο από εξουσιοδοτημένα άτομα κατά τις εργάσιμες ώρες. Σήμερα, η αποθήκευση και η διαχείριση πληροφοριών πραγματοποιείται σε μεγάλο βαθμό ψηφιακά, μέσω προηγμένων τεχνολογικών συστημάτων που ελέγχουν αυτοματοποιημένα την ταυτότητα των χρηστών, ανεξαρτήτως τόπου και χρόνου πρόσβασης.

Παράλληλα, η μετάβαση από τις έντυπες μορφές επικοινωνίας στο ηλεκτρονικό ταχυδρομείο και τις διαδικτυακές συνομιλίες έχει οδηγήσει στη διακίνηση μεγάλου όγκου ευαίσθητων πληροφοριών μέσω διαδικτυακά συνδεδεμένων διακομιστών, αυξάνοντας την έκθεσή τους σε κυβερνοεπιθέσεις. Αντίστοιχα, η ψηφιοποίηση του οπτικοακουστικού περιεχομένου έχει δημιουργήσει νέες προκλήσεις στον τομέα της ασφάλειας. Ενώ στο παρελθόν φωτογραφίες και βίντεο αποθηκεύονταν σε φυσικά μέσα, όπως φιλμ και αρνητικά, σήμερα η συντριπτική πλειονότητα αυτών υφίσταται σε ψηφιακή μορφή.

Στο πλαίσιο αυτό, η εκτεταμένη ψηφιοποίηση των πληροφοριών έχει διευκολύνει τη δράση κυβερνοεγκληματιών, οι οποίοι μπορούν να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση σε λογαριασμούς, συστήματα αποθήκευσης ή διαδικτυακές πλατφόρμες και να υποκλέψουν ή να διαρρεύσουν προσωπικό οπτικοακουστικό υλικό. Παράλληλα, η μετάβαση από τη φυσική στη διαδικτυακή μετάδοση περιεχομένου έχει ενισχύσει φαινόμενα πειρατείας, επιτρέποντας τη μαζική αντιγραφή και παράνομη διανομή ταινιών και τηλεοπτικών σειρών μέσω ιστοσελίδων, οι οποίες συχνά λειτουργούν και ως φορείς κακόβουλου λογισμικού.

Η συνεχής εξέλιξη της τεχνολογίας καθιστά, συνεπώς, αναγκαία τη διαρκή προσαρμογή της κυβερνοασφάλειας, προκειμένου να αντιμετωπίζονται αποτελεσματικά οι νέες απειλές που αναδύονται στο σύγχρονο ψηφιακό περιβάλλον. Άλλωστε, πριν από μερικές δεκαετίες, φάνταζε αδιανόητο ότι ένας ψηφιακός εισβολέας,

ευρισκόμενος σε οποιοδήποτε σημείο του κόσμου, θα μπορούσε να διαταράξει τη λειτουργία μιας επιχείρησης, να επηρεάσει πολιτικές διαδικασίες ή ακόμη και να αποσπάσει χρηματικά ποσά. Η απουσία φυσικής έκθεσης των κυβερνοεγκληματιών στον χώρο τέλεσης της πράξης, σε συνδυασμό με τη δυνατότητα ανώνυμης ή ψευδώνυμης δραστηριοποίησής τους στο διαδίκτυο, μειώνει σημαντικά τον κίνδυνο άμεσου εντοπισμού και σύλληψής τους, γεγονός που καθιστά το κυβερνοέγκλημα ιδιαίτερα ελκυστικό σε σύγκριση με παραδοσιακές μορφές εγκληματικότητας.

Επιπλέον, η ραγδαία ανάπτυξη των ψηφιακών τραπεζικών συναλλαγών και του ηλεκτρονικού εμπορίου έχει προσελκύσει ακόμη περισσότερους παραδοσιακούς εγκληματίες, οι οποίοι στρέφονται στον κυβερνοχώρο ως εναλλακτικό πεδίο εγκληματικής δραστηριότητας. Περαιτέρω, η ταχεία εξάπλωση των κρυπτονομισμάτων κατά την τελευταία δεκαετία έχει δημιουργήσει νέες δυνατότητες για την ανάπτυξη παράνομων δραστηριοτήτων στον ψηφιακό χώρο, καθώς η σχετική ανωνυμία των συναλλαγών μπορεί, μεταξύ άλλων, να διευκολύνει πρακτικές νομιμοποίησης εσόδων από παράνομες δραστηριότητες. Το στοιχείο αυτό διαφοροποιείται από το παραδοσιακό τραπεζικό σύστημα, στο οποίο οι συναλλαγές υπόκεινται σε αυξημένους μηχανισμούς ιχνηλασιμότητας και ελέγχου.

Ακόμη, η εμφάνιση των έξυπνων συσκευών και του Διαδικτύου των Πραγμάτων (Internet of Things – IoT), το οποίο περιλαμβάνει συσκευές συνδεδεμένες στο διαδίκτυο που δεν αποτελούν παραδοσιακούς υπολογιστές, έχει οδηγήσει σε ταχεία εξάπλωση αυτών των τεχνολογιών. Ο συνεχώς αυξανόμενος αριθμός τους, σε συνδυασμό με την αντικατάσταση παλαιότερων μηχανημάτων από διασυνδεδεμένες συσκευές, δημιουργεί πρόσθετες προκλήσεις στον τομέα της ασφάλειας, καθώς καθίσταται δυνατή η απομακρυσμένη πρόσβαση και ο έλεγχός τους από τρίτους, ανεξαρτήτως γεωγραφικής θέσης.

Πέραν των εγκληματικών απειλών, η εκτεταμένη ψηφιοποίηση έχει επιφέρει σημαντικές συνέπειες και σε κοινωνικοπολιτικό επίπεδο. Η ραγδαία αύξηση των διαδικτυακών πληροφοριών και η δυνατότητα πραγματοποίησης κυβερνοεπιθέσεων σε παγκόσμια κλίμακα έχουν ενισχύσει τις δυνατότητες κρατικής παρακολούθησης, επιτρέποντας στις κυβερνήσεις να παρακολουθούν όχι μόνο τους πολίτες τους, αλλά και άτομα εκτός των εθνικών τους συνόρων. Καθώς ολοένα και περισσότερες

επιχειρηματικές, προσωπικές και κοινωνικές δραστηριότητες μεταφέρονται στον ψηφιακό χώρο, καθίσταται δυνατή η συλλογή και επεξεργασία μεγάλων ποσοτήτων δεδομένων με χαμηλότερο κόστος και μεγαλύτερη ευχέρεια σε σύγκριση με το παρελθόν.

Η αυξημένη αλληλεπίδραση στο διαδίκτυο έχει, επιπλέον, ενισχύσει τη διάδοση μορφών ψηφιακού ακτιβισμού, παρέχοντας τη δυνατότητα ενημέρωσης και συμμετοχής σε κοινωνικά και πολιτικά ζητήματα σε παγκόσμιο επίπεδο. Υπό τις συνθήκες αυτές, άτομα που διαφωνούν με κυβερνητικές αποφάσεις μπορούν να εκφράζουν τη στάση τους και να αναλαμβάνουν δράση ανεξαρτήτως της φυσικής τους απόστασης από το επίκεντρο των εξελίξεων.

Τέλος, παρότι η έννοια της ασφάλειας στο διαδίκτυο εμφανίζεται ως ενιαία, η πρακτική εφαρμογή της διαφοροποιείται ανάλογα με τις ανάγκες και τα χαρακτηριστικά κάθε χρήστη ή οργανισμού. Ένας απλός χρήστης που επιδιώκει την ασφάλεια των λογαριασμών του στα μέσα κοινωνικής δικτύωσης δεν υιοθετεί τις ίδιες μεθόδους με έναν κρατικό φορέα που διαχειρίζεται ευαίσθητες πληροφορίες. Για τους ιδιώτες, η διαδικτυακή ασφάλεια επικεντρώνεται κυρίως στην προστασία των προσωπικών δεδομένων και στην αποτροπή κακόβουλων επιθέσεων στις συσκευές τους. Οι μικρότερες επιχειρήσεις δίνουν έμφαση στην ασφαλή διεκπεραίωση οικονομικών συναλλαγών και στην προστασία των δεδομένων των πελατών τους, ενώ οι μεγάλες εταιρείες με εκτεταμένες ψηφιακές υποδομές εστιάζουν στην ασφάλεια των διακομιστών και των συστημάτων αποθήκευσης δεδομένων, με σκοπό την αποτροπή παραβιάσεων ασφαλείας.

1.2 Οι βασικές αρχές της κυβερνοασφάλειας

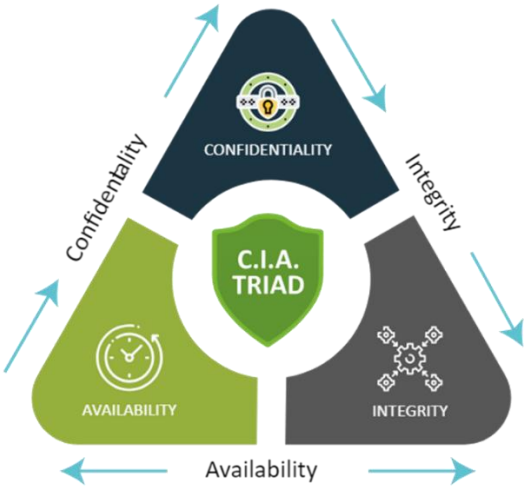
Η τριάδα της CIA (CIA Triad) στην Κυβερνοασφάλεια αναφέρεται στις τρεις (3) βασικές αρχές που διασφαλίζουν την προστασία και ασφάλεια των πληροφοριών & δεδομένων:

Confidentiality (Εμπιστευτικότητα) – Εξασφαλίζει ότι η πρόσβαση στα δεδομένα επιτρέπεται μόνο σε εξουσιοδοτημένα άτομα.

Integrity (Ακεραιότητα) – Διασφαλίζει ότι τα δεδομένα παραμένουν ακριβή και αμετάβλητα χωρίς μη εξουσιοδοτημένες τροποποιήσεις.

Availability (Διαθεσιμότητα) – Εγγυάται ότι τα δεδομένα και τα συστήματα είναι διαθέσιμα στους εξουσιοδοτημένους χρήστες, όταν απαιτείται.

Αυτές οι τρεις αρχές αποτελούν το θεμέλιο της ασφάλειας πληροφοριών και χρησιμοποιούνται για τον σχεδιασμό και την αξιολόγηση των στρατηγικών κυβερνοασφάλειας.



Οι τρείς αρχές της Ασφάλειας Πληροφοριών

Ας δούμε όμως αναλυτικά κάθε έννοια:

1.2.1 Εμπιστευτικότητα (Confidentiality)

Η εμπιστευτικότητα αναφέρεται στην προστασία των ευαίσθητων πληροφοριών, εξασφαλίζοντας ότι αυτές δεν θα αποκαλυφθούν ή θα διανεμηθούν σε μη εξουσιοδοτημένα άτομα ή οργανισμούς. Ο στόχος είναι να διασφαλιστεί ότι μόνο εκείνοι που έχουν την κατάλληλη εξουσιοδότηση θα έχουν πρόσβαση σε αυτές τις πληροφορίες. Μια παραβίαση της εμπιστευτικότητας συμβαίνει, όταν εμπιστευτικά δεδομένα αποκαλύπτονται, είτε σκοπίμως είτε κατά λάθος, σε άτομα ή φορείς χωρίς τη συγκατάθεση του κατόχου τους.

Για παράδειγμα, αν ένας χάκερ καταφέρει να παραβιάσει τη βάση δεδομένων ενός οργανισμού και αποκτήσει πρόσβαση σε προσωπικά δεδομένα πελατών, παραβιάζεται η εμπιστευτικότητα και αυτό μπορεί να οδηγήσει σε οικονομικές ζημιές για τα θύματα και να πλήξει την εμπιστοσύνη τους. Οι πληροφορίες που συνήθως

προστατεύονται περιλαμβάνουν προσωπικά δεδομένα, αριθμούς πιστωτικών καρτών, τραπεζικούς λογαριασμούς, ιατρικά αρχεία και εμπορικά μυστικά. Μερικοί από τους κυριότερους κινδύνους παραβίασης της εμπιστευτικότητας περιλαμβάνουν:

i. την κλοπή φορητών υπολογιστών,

ii. την ακατάλληλη πρόσβαση σε υπολογιστές που περιέχουν εμπιστευτικά δεδομένα,

iii. την κακόβουλη χρήση λογισμικού από χάκερ,

iv. την παράνομη πρόσβαση από υπαλλήλους και συνεργάτες και

v. τη χρήση δεδομένων για προσωπικό όφελος.

Είναι σημαντικό να αναφερθεί ότι οι κύριες αιτίες για παραβίαση της εμπιστευτικότητας προέρχονται από ανθρώπινα λάθη και υπαλλήλους που εργάζονται στο εσωτερικό του οργανισμού και έχουν πρόσβαση σε εταιρικές πληροφορίες και δεδομένα. Αν και οι χάκερς αποτελούν εξίσου σοβαρή απειλή, ο κίνδυνος από αυτούς μπορεί να μειωθεί σημαντικά με την εφαρμογή των κατάλληλων μέτρων ασφάλειας, που προστατεύουν τα δεδομένα από μη εξουσιοδοτημένες προσβάσεις.

1.2.2 **Ακεραιότητα (Integrity)**

Η ακεραιότητα αναφέρεται στις διαδικασίες και τα εργαλεία που εξασφαλίζουν ότι τα δεδομένα παραμένουν ακριβή και πλήρη κατά τη διάρκεια όλου του κύκλου ζωής τους. Διασφαλίζοντας την ακεραιότητα, εξασφαλίζουμε ότι τα δεδομένα δεν αλλοιώνονται ή χάνονται ακούσια ή εκούσια:

•Ακριβή σημαίνει ότι τα δεδομένα δεν τροποποιούνται με μη εξουσιοδοτημένο τρόπο, είτε από ανθρώπινα λάθη είτε από τεχνικές βλάβες.

•Πλήρη δεδομένα είναι αυτά που δεν έχουν χάσει καμία πληροφορία, είτε από εξωτερικές παρεμβάσεις είτε από τεχνικά προβλήματα.

Η ακεραιότητα περιλαμβάνει και την έννοια της μη αμφισβήτησης (Non repudiation), δηλαδή ότι τα δεδομένα πρέπει να προστατεύονται με τέτοιον τρόπο ώστε να μην μπορεί κανείς να αμφισβητήσει την αυθεντικότητά τους. Γι' αυτό, τα δεδομένα θα πρέπει να είναι κρυπτογραφημένα τόσο κατά την αποθήκευση (data at rest) όσο και κατά

τη μεταφορά τους (data in motion), ώστε να παραμένουν ασφαλή και να διασφαλίζεται η ακεραιότητά τους.

Όταν παραβιάζεται η ακεραιότητα, τα δεδομένα μπορεί να παραποιηθούν, να καταστραφούν ή να καταστούν άχρηστα. Για παράδειγμα, οι χάκερς μπορούν να παραβιάσουν την ακεραιότητα των δεδομένων μέσω:

- Εγκατάστασης κακόβουλου λογισμικού στους υπολογιστές.
- Κρυπτογράφησης δεδομένων με σκοπό τον εκβιασμό.
- Τροποποίησης των δεδομένων ή παραποίησής τους.
- Εισαγωγής ιών που επηρεάζουν τα δεδομένα.
- Κακόβουλων ενεργειών από εσωτερικούς υπαλλήλους.
- Επιθέσεων που αλλάζουν δεδομένα κατά τη μετάδοσή τους, όπως στις επιθέσεις "man-in-the-middle".

Κάθε ενέργεια που επηρεάζει τη συνέπεια ή την ακρίβεια των δεδομένων αποτελεί παραβίαση της ακεραιότητας.

1.2.3 **Διαθεσιμότητα (Availability)**

Η διαθεσιμότητα αφορά τη διασφάλιση ότι οι εξουσιοδοτημένοι χρήστες μπορούν να έχουν πρόσβαση στα δεδομένα και τις υπηρεσίες που χρειάζονται χωρίς καθυστερήσεις ή διακοπές. Για να επιτευχθεί αυτό, τα συστήματα αποθήκευσης και επεξεργασίας πληροφοριών, οι μηχανισμοί επικοινωνίας και οι έλεγχοι ασφαλείας πρέπει να λειτουργούν σωστά και να πληρούν συγκεκριμένα πρότυπα αξιοπιστίας. Αν, για παράδειγμα, ένας υπολογιστής παρουσιάσει βλάβη ή το δίκτυο παρουσιάσει χαμηλή ταχύτητα, η πρόσβαση στα δεδομένα μπορεί να καταστεί αδύνατη, γεγονός που επηρεάζει τη λειτουργικότητα των υπηρεσιών.

Παρότι συχνά η διαθεσιμότητα θεωρείται λιγότερο κρίσιμη σε σχέση με την εμπιστευτικότητα και την ακεραιότητα, στην πραγματικότητα αποτελεί βασικό στοιχείο της ασφάλειας πληροφοριών. Η διατήρησή της είναι απαιτητική, καθώς απαιτεί συνεργασία μεταξύ διαφόρων ειδικοτήτων, συμπεριλαμβανομένων μηχανικών συστημάτων, διαχειριστών δικτύων και ειδικών ασφαλείας.

Η διαθεσιμότητα μπορεί να διαταραχθεί είτε λόγω τεχνικών προβλημάτων είτε εξαιτίας κακόβουλων ενεργειών. Επιθέσεις, όπως το DoS (Denial of Service), στοχεύουν στη δημιουργία τεχνητού φόρτου σε ένα σύστημα, εμποδίζοντας τους νόμιμους χρήστες από το να το χρησιμοποιήσουν. Οι εισβολές σε δίκτυα, από την άλλη, επιτρέπουν σε επιτιθέμενους να πάρουν τον έλεγχο κρίσιμων υποδομών, αποτρέποντας έτσι την πρόσβαση σε σημαντικές υπηρεσίες.

Βασικοί παράγοντες που μπορούν να οδηγήσουν σε διακοπή της διαθεσιμότητας είναι: Βλάβες ή δυσλειτουργίες υλικού, Σφάλματα λογισμικού, Υπερφόρτωση του δικτύου, Στοχευμένες κυβερνοεπιθέσεις, όπως DoS

Αν και οι διακοπές στις υπηρεσίες μπορεί να προκληθούν από τυχαίους παράγοντες, όπως τεχνικές αστοχίες ή περιβαλλοντικές συνθήκες, όταν προέρχονται από εσκεμμένες ενέργειες εισβολέων, αντιμετωπίζονται ως επιθέσεις που αποσκοπούν στην αποσταθεροποίηση ενός συστήματος. Σε αυτές τις περιπτώσεις, χρησιμοποιούνται συχνά προηγμένες τεχνικές και μεγάλος όγκος υπολογιστικής ισχύος για να επιτευχθεί η διακοπή της υπηρεσίας.

2. ΜΟΡΦΕΣ ΚΑΙ ΤΥΠΟΙ ΚΥΒΕΡΝΟΕΠΙΘΕΣΕΩΝ ΚΑΙ ΟΙ ΕΠΙΠΤΩΣΕΙΣ ΤΟΥΣ ΣΤΗΝ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ

2.1 Κύριες μορφές και τύποι επιθέσεων στον κυβερνοχώρο κατά των επιχειρήσεων

Οι απειλές για την ασφάλεια στον κυβερνοχώρο συνεχώς αυξάνονται καθώς νέες τεχνολογίες και τάσεις δημιουργούν περισσότερες ευκαιρίες για κυβερνοεγκληματίες. Η συνεχώς αυξανόμενη διαδικτυακή και ψηφιακή παρουσία συντείνει στη μετάβαση από τις παραδοσιακές υποδομές σε διαδικτυακές λύσεις και λύσεις που βασίζονται στο υπολογιστικό νέφος (cloud computing), στην προηγμένη διασυνδεσιμότητα και την εκμετάλλευση νέων χαρακτηριστικών των αναδυόμενων τεχνολογιών, όπως η Τεχνητή Νοημοσύνη (Artificial Intelligence - AI).

Στον τομέα της κυβερνοασφάλειας υφίσταται σημαντική αύξηση της πολυπλοκότητας των επιθέσεων. Η ασφάλεια πληροφοριών είναι η διαδικασία προστασίας των προσωπικών και εταιρικών δεδομένων και αποτροπής της πρόσβασης σε αυτά, της τροποποίησης ή της απώλειάς τους, μέσω μη εξουσιοδοτημένης πρόσβασης. Αυτό περιλαμβάνει την προστασία των δεδομένων από επιθέσεις σε πληροφοριακά συστήματα όπου αυτά (τα δεδομένα) φυλάσσονται.

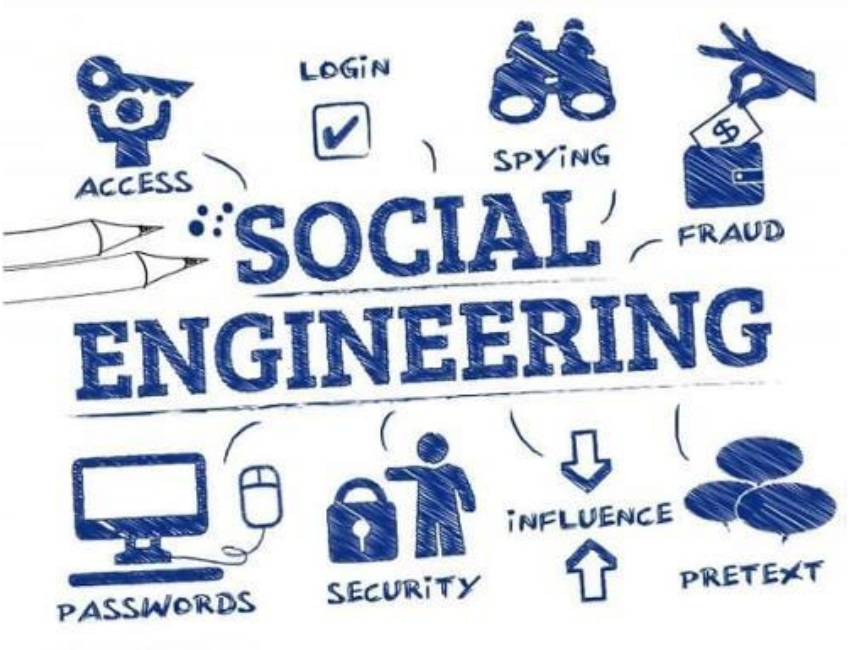
Ακολουθεί μια ενδεικτική λίστα και ταξινόμηση με τους περισσότερο διαδεδομένους κινδύνους και απειλές για την ασφάλεια των δεδομένων και των πληροφοριών για τις σύγχρονες επιχειρήσεις και τους οργανισμούς.

2.2 Κοινωνική μηχανική (social engineering)

Ο όρος κοινωνική μηχανική (social engineering) αναφέρεται σε όλες εκείνες τις τεχνικές που στοχεύουν στο να ωθήσουν έναν στόχο στην αποκάλυψη συγκεκριμένων πληροφοριών ή στην εκτέλεση μιας συγκεκριμένης ενέργειας για παράνομους λόγους. Η κοινωνική μηχανική δεν σταματά μόνο στη συνομιλία με το θύμα-στόχο, αλλά μπορεί επίσης να συνδυαστεί με άλλες τεχνικές που περιγράφονται σε επόμενα κεφάλαια, όπως επιθέσεις ηλεκτρονικού ψαρέματος (phishing), επιθέσεις κατάληψης συστήματος (compromised system attacks) και άλλες συναφείς ενέργειες.

Η κοινωνική μηχανική ορίζεται ως η ψυχολογική χειραγώγηση της ανθρώπινης συμπεριφοράς με στόχο να επηρεάσει τους ανθρώπους να ενεργήσουν με

συγκεκριμένους τρόπους ή να αποκαλύψουν εμπιστευτικές πληροφορίες. Είναι μια τεχνική που εκμεταλλεύεται την τρόπο με τον οποίο λειτουργεί ο άνθρωπος, το πώς αντιλαμβάνεται το περιβάλλον του βάσει των εμπειριών του, καθώς και θεμελιώδη ένστικτα, όπως η εμπιστοσύνη, η εξουσία, η επείγουσα ανάγκη, η εξοικείωση και άλλα, προκειμένου να συλλέξει πληροφορίες, να εξαπατήσει γενικότερα ή να αποκτήσει πρόσβαση σε συστήματα. Η κοινωνική μηχανική είναι το «αγαπημένο» εργαλείο των εγκληματιών του κυβερνοχώρου, οι οποίοι σε αρκετές περιπτώσεις χρησιμοποιούν πλατφόρμες κοινωνικής δικτύωσης και ηλεκτρονικού ταχυδρομείου για την επίτευξη του στόχου τους



Κοινωνική Μηχανική (Social Engineering)

Η επιτυχής εκτέλεση της κοινωνικής μηχανικής απαιτεί λεπτομερή συλλογή πληροφοριών σχετικά με το θύμα, ώστε να γίνει πιο πειστική και αληθοφανής η προσέγγισή του. Αυτή η διαδικασία συλλογής πληροφοριών, που αναφέρεται ως doxing (το doxing αποτελεί σοβαρή απειλή για την ασφάλεια επιχειρήσεων και οργανισμών, καθώς μπορεί να αποκαλύψει ευαίσθητες πληροφορίες σχετικά με τους υπαλλήλους ή τα στελέχη τους), διευκολύνεται μέσω μιας τεχνικής, γνωστής ως OSINT (Open-source intelligence) δηλαδή συλλογή δεδομένων από ανοιχτές πηγές του Διαδικτύου.

Μετά τη συλλογή πληροφοριών σχετικά με τον στόχο, το επόμενο κρίσιμο βήμα για τον δράστη της κοινωνικής μηχανικής είναι η ανάπτυξη μιας συναισθηματικής ή ψυχολογικής σύνδεσης με το θύμα. Αυτή η διαδικασία βασίζεται στην αξιοποίηση συγκεκριμένων αρχών ψυχολογικής επιρροής, οι οποίες έχουν αποδειχθεί ιδιαίτερα αποτελεσματικές στην παραπλάνηση των θυμάτων.

Μια από τις βασικότερες τεχνικές είναι η άσκηση εξουσίας, όπου ο επιτιθέμενος προσποιείται ότι κατέχει θέση κύρους ή αρμοδιότητας, ενισχύοντας τη συμμόρφωση του στόχου μέσω της αυθεντίας του. Αυτό μπορεί να επιτευχθεί τόσο μέσω λεκτικής επικοινωνίας όσο και μέσω πλαστογραφημένων μηνυμάτων, όπως email που φέρουν ψεύτικες ιδιότητες (π.χ. "Διευθυντής Πληροφορικής").

Η τεχνική του εκφοβισμού συνδέεται συχνά με την εξουσία και περιλαμβάνει την πρόκληση πίεσης ή φόβου στο θύμα, είτε μέσω απειλών είτε μέσω έντονης επιβολής, ώστε να το ωθήσει σε ενέργειες που εξυπηρετούν τον δράστη. Η αρχή της συναίνεσης εκμεταλλεύεται τη φυσική ανθρώπινη τάση για κοινωνική συμμόρφωση, βασιζόμενη στην ιδέα ότι “κι άλλοι το έκαναν ήδη” — δηλαδή, παρουσιάζοντας ψευδείς μαρτυρίες ή παραδείγματα ώστε το θύμα να θεωρήσει την ενέργεια ως αποδεκτή ή συνηθισμένη. Παράλληλα, η οικειότητα χρησιμοποιείται για να καλλιεργήσει ένα αίσθημα ασφάλειας, καθώς οι άνθρωποι έχουν την τάση να εμπιστεύονται άτομα ή οντότητες που φαίνονται γνώριμα, όπως κάποιος «γνωστός από το τμήμα» ή «συνεργάτης από άλλη υπηρεσία». Η εμπιστοσύνη είναι μια πιο σύνθετη τεχνική, όπου ο δράστης επενδύει χρόνο και προσπάθεια για να δημιουργήσει μια σχέση που βασίζεται στην επίπλαστη αξιοπιστία και φιλικότητα, με σκοπό την εκμετάλλευση του θύματος σε μεταγενέστερο στάδιο. Ακόμη, η αίσθηση επείγοντος είναι ένα συχνό εργαλείο πίεσης: ο επιτιθέμενος παρουσιάζει μια κατάσταση ως επείγουσα, αναγκάζοντας το θύμα να αντιδράσει άμεσα και παρορμητικά, χωρίς να έχει τον απαραίτητο χρόνο για να αξιολογήσει τους κινδύνους. Τέλος, το ηλεκτρονικό ψάρεμα (phishing) αποτελεί μια ιδιαίτερα διαδεδομένη μορφή κοινωνικής μηχανικής, με στόχο την υποκλοπή διαπιστευτηρίων ή ευαίσθητων πληροφοριών. Συχνά, τέτοιες επιθέσεις λαμβάνουν τη μορφή ψευδών e-mail ή ιστοσελίδων που μιμούνται νόμιμους οργανισμούς.

2.3 Ηλεκτρονικό ψάρεμα (phishing)

Μία από τις πιο διαδεδομένες απειλές που αντιμετωπίζουν οι επιχειρήσεις είναι οι επιθέσεις ηλεκτρονικού ψαρέματος (phishing). Αυτές οι παραπλανητικές τακτικές περιλαμβάνουν κακόβουλες οντότητες που παρουσιάζονται ως αξιόπιστες, ώστε να χειραγωγήσουν άτομα προκειμένου εκείνα να αποκαλύψουν ευαίσθητες πληροφορίες. Οι επιχειρήσεις και οι οργανισμοί, με το ποικιλόμορφο εργατικό δυναμικό τους και τους -ανάλογα με την περίπτωση- περιορισμένους πόρους για εκτεταμένη εκπαίδευση στον κυβερνοχώρο, ενδέχεται να είναι ιδιαίτερα ευάλωτοι σε τέτοιους τύπους επιθέσεων. Μια επιτυχημένη επίθεση ηλεκτρονικού ψαρέματος μπορεί να οδηγήσει σε μη εξουσιοδοτημένη πρόσβαση σε κρίσιμα συστήματα, να διακυβεύσει ευαίσθητα δεδομένα και να προκαλέσει δυνητικά ανεπανόρθωτη ζημιά στην επιχείρηση.

Οι επιθέσεις αυτού του τύπου μπορούν να ταξινομηθούν στις ακόλουθες κατηγορίες:

Spear Phishing (εστιασμένο ηλεκτρονικό ψάρεμα): Αυτές οι επιθέσεις συχνά περιλαμβάνουν εκτεταμένη έρευνα για τον κάθε στόχο. Το spear phishing περιλαμβάνει τη δημιουργία εξαιρετικά εξατομικευμένων και πειστικών μηνυμάτων ηλεκτρονικού ταχυδρομείου προκειμένου να εξαπατηθεί ο παραλήπτης και να ενεργήσει για λογαριασμό του εισβολέα.

Whale Phising (κυνήγι «φαλαινών»): Μια παραλλαγή του πρώτου τύπου με την ιδιαιτερότητα ότι η συγκεκριμένη στοχεύει συγκεκριμένα άτομα υψηλού προφίλ (μεγάλα ψάρια). Σε αυτές τις επιθέσεις, οι εγκληματίες του κυβερνοχώρου υποδύονται ένα ανώτερο στέλεχος ή μια αξιόπιστη προσωπικότητα εντός του οργανισμού και στέλνουν ψευδή μηνύματα ηλεκτρονικού ταχυδρομείου σε υπαλλήλους, προμηθευτές ή επιχειρηματικούς εταίρους. Σε αυτά τα μηνύματα ηλεκτρονικού ταχυδρομείου συνήθως ζητείται επείγουσα δράση, όπως τραπεζικά εμβάσματα ή αποκάλυψη ευαίσθητων πληροφοριών. Οι επιθέσεις αυτές είναι συχνά εξελιγμένες και προσεκτικά κατασκευασμένες ώστε να μιμούνται το στυλ επικοινωνίας και το επίπεδο εξουσίας του ατόμου που υποδύονται, κάτι που καθιστά έτσι δύσκολο τον εντοπισμό τους.

Vishing phishing (φωνητικό ηλεκτρονικό ψάρεμα): Αυτός ο όρος αναφέρεται στο ηλεκτρονικό ψάρεμα μέσω τηλεφώνου, στο πλαίσιο του οποίου οι προσπάθειες εξαπάτησης πραγματοποιούνται μέσω φωνητικής επικοινωνίας. Σε αυτά τα συστήματα,

οι εγκληματίες του κυβερνοχώρου υποδύονται συνήθως αξιόπιστες οντότητες, όπως τράπεζες ή κυβερνητικές υπηρεσίες, εκμεταλλευόμενοι τακτικές κοινωνικής μηχανικής για να χειραγωγήσουν τα θύματα.

Smishing (ηλεκτρονικό ψάρεμα μέσω μηνυμάτων SMS): Αυτή η μέθοδος χρησιμοποιείται συνήθως για την αποστολή κακόβουλου λογισμικού σε κινητές συσκευές ή για την κλοπή διαπιστευτηρίων. Αυτά τα μηνύματα συχνά περιέχουν επείγοντα αιτήματα ή προσφορές που έχουν σχεδιαστεί για να προτρέπουν τους παραλήπτες να κάνουν κλικ σε κακόβουλους συνδέσμους, να καλούν ψευδείς αριθμούς τηλεφώνου ή να παρέχουν ευαίσθητες πληροφορίες, όπως διαπιστευτήρια λογαριασμού ή προσωπικά στοιχεία.

Ηλεκτρονικό ψάρεμα για επίθεση σε ηλεκτρονικό ταχυδρομείο επιχειρήσεων: Αυτός ο όρος περιλαμβάνει απάτες που συνήθως συνεπάγονται παραβίαση νόμιμων εταιρικών λογαριασμών ηλεκτρονικού ταχυδρομείου. Ο στόχος είναι να εξαπατηθεί το θύμα ώστε να εγκρίνει μη εξουσιοδοτημένες μεταφορές αγαθών, να αποκαλύψει εμπιστευτικές πληροφορίες και, σε ορισμένες περιπτώσεις, να εγκαταστήσει κακόβουλο λογισμικό, όπως keyloggers (καταγραφείς πληκτρολόγησης). Αυτού του είδους οι επιθέσεις συχνά απαιτούν εκτεταμένη έρευνα σε ένα σύστημα εταιρικής επικοινωνίας προκειμένου να μιμηθούν αποτελεσματικά τις επικοινωνίες εντός οργανισμού, όπως για παράδειγμα μεταξύ ενός ατόμου υψηλά ιστάμενου στην ιεραρχία το οποίο υποβάλλει επείγον αίτημα σε έναν εργαζόμενο του τμήματος για τραπεζικό έμβασμα ή για παροχή ευαίσθητων πληροφοριών.

2.4 Κακόβουλο λογισμικό (malware)

Το κακόβουλο λογισμικό ορίζεται ως ένα πρόγραμμα που έχει σχεδιαστεί για να εισβάλλει σε έναν υπολογιστή, διακομιστή ή σε δίκτυο υπολογιστών και να προχωρά σε μη εξουσιοδοτημένη απόκτηση ευαίσθητων πληροφοριών και κρίσιμων δεδομένων, καθώς και να διεισδύει σε πληροφοριακά συστήματα. Αυτό το είδος λογισμικού συνιστά μια πολύπλευρη απειλή, η οποία έχει ως στόχο να θέσει σε κίνδυνο την ψηφιακή ασφάλεια όχι μόνο προκαλώντας λειτουργικές διακοπές αλλά και θέτοντας σε κίνδυνο την εμπιστευτικότητα και την ακεραιότητα των ιδιωτικών πληροφοριών.

Πολλές φορές το κακόβουλο λογισμικό έχει την ικανότητά αναπαραγωγής, διάδοσης και αυτοεκτέλεσης, καταστρέφοντας υπολογιστικά συστήματα. Μια τέτοια καταστροφή ωστόσο μπορεί να επιφέρει εκτεταμένες συνέπειες, επηρεάζοντας τις βασικές πτυχές της ασφάλειας των δεδομένων. Η αναπαραγωγή ξεχωρίζει ως βασικό χαρακτηριστικό των περισσότερων κακόβουλων προγραμμάτων, διασφαλίζοντας την επιβίωση τους εντός των υπολογιστικών συστημάτων. Σε ορισμένες περιπτώσεις μάλιστα, η ακατάπαυστη αναπαραγωγή κακόβουλου λογισμικού μπορεί να οδηγήσει στην εξάντληση των κρίσιμων πόρων του υπολογιστή, όπως ο χώρος στον σκληρό δίσκο και η μνήμη τυχαίας προσπέλασης (RAM).

Επίσης η ιδιότητα της απόκρυψης χρησιμοποιείται ευρέως από πολλούς τύπους κακόβουλων λογισμικών προγραμμάτων προκειμένου να αποφύγουν τον εντοπισμό από άλλα προγράμματα που λειτουργούν αποτρεπτικά εναντίον τους. Αυτό επιτυγχάνεται συχνά μέσω τεχνικών, όπως ο πολυμορφισμός ή ο μεταμορφισμός, δια των οποίων το κακόβουλο λογισμικό μπορεί να αλλάξει τη δομή του κώδικά του, γεγονός που καθιστά δύσκολη την αναγνώριση και την καταπολέμησή του από τα παραδοσιακά μέτρα ασφαλείας.

Ωστόσο η πλέον κοινή μέθοδος που χρησιμοποιείται από τα κακόβουλα λογισμικά για τη μόλυνση ενός συστήματος περιλαμβάνει την μεταφορά του κακόβουλου προγράμματος από μια παραβιασμένη συσκευή σε μια μη μολυσμένη. Αυτή η μετάδοση πραγματοποιείται μέσω τοπικών ή δικτυακών συστημάτων αρχείων, επηρεάζοντας δεδομένα, εκτελέσιμα αρχεία ή καταναλώνοντας εύρος ζώνης δικτύου (Bandwidth). Οι ευπάθειες του λειτουργικού συστήματος και τα σφάλματα λογισμικού (bugs) χρησιμεύουν ως σημεία εισόδου. Μόλις επέλθει η μόλυνση, το κακόβουλο λογισμικό μπορεί να ξεκινήσει τον κύκλο ζωής του στο ίδιο σύστημα ή να αποκτήσει απομακρυσμένο έλεγχο και σε άλλα συστήματα, κάτι που διευκολύνει τις λειτουργίες μόλυνσης σε αυτά. Αυτή η περίπλοκη δράση αναδεικνύει την πολύπλευρη φύση και ικανότητα του κακόβουλου λογισμικού να θέτει σε κίνδυνο τα ψηφιακά συστήματα.

Ως εκ τούτου, το κακόβουλο λογισμικό μπορεί να οριστεί ως οποιοδήποτε λογισμικό προορίζεται να εκτελέσει μια κακόβουλη και μη εξουσιοδοτημένη διαδικασία, η οποία θα έχει αρνητικό αντίκτυπο στην εμπιστευτικότητα, την ακεραιότητα ή τη διαθεσιμότητα ενός πληροφοριακού συστήματος.

Ειδικότερα τα κακόβουλα λογισμικά μπορούν να έχουν διάφορες δυνατότητες ανάλογα με τον στόχο του δημιουργού τους. Για παράδειγμα, τα RATs (Remote Access Trojans/Tools) είναι κακόβουλα προγράμματα που επιτρέπουν σε έναν επιτιθέμενο τον απομακρυσμένο έλεγχο ενός μολυσμένου συστήματος. Από την άλλη πλευρά οι συσκευές skimming (συσκευές υποκλοπής δεδομένων) έχουν σχεδιαστεί για να υποκλέπτουν πληροφορίες από πιστωτικές κάρτες, ενώ τα botnets (συντομογραφία του «robot networks») αποτελούν δίκτυα υπολογιστών που έχουν μολυνθεί από κακόβουλο λογισμικό και ελέγχονται από διακομιστές Command and Control (C&C). Για λόγους πληρότητας ανάλυσης της εν λόγω μορφής κυβερνοεπίθεσης, ακολουθεί αναλυτική περιγραφή των πλέον διαδεδομένων κατηγοριών κακόβουλου λογισμικού.

2.4.1 Spyware

Το spyware είναι ένας τύπος κακόβουλου λογισμικού που παρακολουθεί τις διαδικτυακές δραστηριότητες των χρηστών με στόχο τη συλλογή κυρίως οικονομικών δεδομένων, κωδικών πρόσβασης και άλλων ευαίσθητων πληροφοριών. Συνήθως εντοπίζεται σε κοινές επιθέσεις, όπως αυτές που πραγματοποιούνται μέσω διαφημίσεων, μηνυμάτων ηλεκτρονικού ταχυδρομείου ή ιστότοπων. Το κακόβουλο αυτό λογισμικό απαιτεί σύνδεση στο διαδίκτυο για να αποστείλει τις συλλεγόμενες πληροφορίες πίσω στον κυβερνοεγκληματία. Υπάρχουν τέσσερις βασικοί τύποι spyware: keyloggers, password stealers, info stealers και mobile spyware.

Τα keyloggers παρακολουθούν και καταγράφουν κάθε πληκτρολόγηση του χρήστη στο υπολογιστικό σύστημα που χρησιμοποιεί, συλλέγοντας ευαίσθητες πληροφορίες όπως κωδικοί πρόσβασης και προσωπικά δεδομένα. Οι password stealers είναι σχεδιασμένοι να υποκλέπτουν στοιχεία σύνδεσης χρηστών από διάφορους λογαριασμούς, όπως τραπεζικούς λογαριασμούς, λογαριασμούς μέσων κοινωνικής δικτύωσης καθώς και λογαριασμούς ηλεκτρονικών ταχυδρομείων (e-mail accounts). Οι info stealers συλλέγουν δεδομένα όπως το ιστορικό περιήγησης και οι αποθηκευμένοι κωδικοί από τρίτες πηγές. Το mobile spyware εγκαθίσταται μέσω SMS σε κινητές συσκευές χωρίς αλληλεπίδραση από τον χρήστη, επιτρέποντας την μυστική

παρακολούθηση του μέσω μη εξουσιοδοτημένης πρόσβασης στην κάμερα, στο μικρόφωνο, στις τηλεφωνικές κλήσεις και στο ιστορικό αναζήτησης της συσκευής.

2.4.2 Virus

Αυτός είναι ο πιο κοινός τύπος κακόβουλου λογισμικού, ο οποίος έχει το ιδίωμα να κρύβεται στον πηγαίο κώδικα της εφαρμογής που έχει μολυνθεί, μέχρι να ολοκληρώσει την προγραμματισμένη του εργασία. Το λογισμικό αυτό τροποποιεί τις ρυθμίσεις των προγραμμάτων να τα παραβιάσει και να εισαγάγει τον δικό του κώδικά, με αποτέλεσμα όταν ένας χρήστης ενεργοποιήσει μια μολυσμένη εφαρμογή, ο ιός αρχίζει να αναπαράγεται και να εκτελεί την κακόβουλη εργασία του. Να σημειωθεί δε, ότι ο εν λόγω ιός δρα σε τέσσερα στάδια. Το πρώτο είναι αυτό κατά το οποίο το κακόβουλο λογισμικό χρειάζεται ενεργοποίηση από τον χρήστη για να λειτουργήσει. Εν συνεχεία ακολουθεί η διάδοση του, κατά την οποία ο ιός μέσω διαδικασίας κλωνοποίησης μολύνει όσο το δυνατόν περισσότερα μέρη του πληροφοριακού συστήματος. Μάλιστα έχει την δυνατότητα να αναπαράγεται συνεχώς μέχρι να κατακλύσει το σύστημα ή το λογισμικό προστασίας από ιούς. Κατά την τρίτη φάση, ο ιός εκτελεί το προγραμματισμένο του έργο, ενώ κατά το τελευταίο στάδιο εκτέλεσης αποστέλλει πληροφορίες στον χειριστή του.

2.4.3 Rootkit

Το εν λόγω κακόβουλο λογισμικό είναι σχεδιασμένο να επιχειρεί να αποκτήσει μη εξουσιοδοτημένη πρόσβαση σε ένα δίκτυο, χωρίς να γίνει αντιληπτό. Ειδικότερα, σκοπός του είναι να αποκτήσει δικαιώματα διαχειριστή ενός συστήματος, προκειμένου να το ελέγξει και να εγκαταστήσει σε αυτό πρόσθετο κακόβουλο λογισμικό. Χαρακτηριστικό του δε γνώρισμα είναι ότι προσκολλάται συνήθως σε γνήσιο λογισμικό ή σε εφαρμογές για συσκευές κινητής τηλεφωνίας και δεν είναι εύκολο να ανιχνευθεί.

2.4.4 Adware

Αυτός ο τύπος κακόβουλου λογισμικού εμφανίζει αναδυόμενα παράθυρα ή δυναμικές διαφημίσεις χωρίς την συναίνεση του χρήστη, τις οποίες ο τελευταίος καθώς

παρακολουθεί, το λογισμικό αποκτά πρόσβαση σε αρχεία του υπολογιστικού του συστήματος και συλλέγει δεδομένα με σκοπό την κατάρτιση προφίλ του χρήστη. Επίσης το συγκεκριμένο κακόβουλο λογισμικό μπορεί να επιβραδύνει το πρόγραμμα περιήγησης και να το παραβιάσει, τροποποιώντας ρυθμίσεις σε εφαρμογές, όπως στις μηχανές αναζήτησης ή τις γραμμές εργαλείων, προβάλλοντας σελίδες ηλεκτρονικού ψαρέματος ή εγκαθιστώντας δευτερογενές κακόβουλο λογισμικό.

2.4.5 Λυτρισμικό ή λογισμικό κατάληψης συστήματος (ransomware)

Το λυτρισμικό, γνωστό και ως ransomware, είναι ένα ιδιαίτερα επικίνδυνο είδος κακόβουλου λογισμικού (malware) για τις επιχειρήσεις σήμερα, που σχεδιάζεται για να καταλάβει και να «κλειδώσει» τα αρχεία τους ή ακόμα και ολόκληρα τα πληροφοριακά και επικοινωνιακά τους συστήματα καθώς και τις ψηφιακές τους υποδομές του οργανισμού.

Η προσέγγιση που ακολουθεί το ransomware περιλαμβάνει συνήθως την κρυπτογράφηση των αρχείων του χρήστη ή των δεδομένων του δικτύου, καθιστώντας τα μη προσβάσιμα, προκαλώντας τεράστια ζημιά στην λειτουργία μιας επιχείρησης. Προς αποκρυπτογράφηση των δεδομένων και αποκατάσταση της πρόσβασης, ο επιτιθέμενος ζητά την καταβολή ενός ποσού σε κρυπτονομίσματα (όπως Bitcoin ή Monero) ως λύτρα (ransom).

2.4.6 Απειλές σχετιζόμενες με το ηλεκτρονικό ταχυδρομείο (e-mail related threats)

Οι απειλές που σχετίζονται με το ηλεκτρονικό ταχυδρομείο κατατάσσονται σταθερά υψηλά στη λίστα με τις κύριες απειλές για τα υπολογιστικά συστήματα και αναλύθηκαν εκτενώς στις προηγούμενες θεματικές ενότητες. Αυτή η ομάδα απειλών εκμεταλλεύεται τις αδυναμίες στην ανθρώπινη συμπεριφορά σχετικά με τα e-mails και τις ανθρώπινες συνήθειες και στοχεύει στη χειραγώγηση των ατόμων ώστε να πέσουν θύματα επίθεσης. Οι απειλές που σχετίζονται με το ηλεκτρονικό ταχυδρομείο αφορούν σε μικρότερο βαθμό τεχνικές ευπάθειες των συστημάτων πληροφοριών, καθώς βασίζονται κυρίως στην κοινωνική μηχανική, δηλαδή στην ευαισθητοποίηση του τελικού

χρήστη και την εκμετάλλευση της εγγενούς εμπιστοσύνης που δείχνουν οι άνθρωποι κατά τις επικοινωνίες τους μέσω e-mail. Το συγκεκριμένο είδος απειλής παρουσιάζει πολλαπλές εκδοχές με διαφοροποιήσεις ως προς την λειτουργία και την συμπεριφορά του όπως το phishing, το spear-phishing, το whaling, το smishing, το vishing. Ωστόσο στο σημείο αυτό θα πρέπει να σταθούμε στις επιθέσεις που πραγματοποιούντια σε θυρίδες ηλεκτρονικού ταχυδρομείου επιχειρήσεων. Οι επιθέσεις αυτές ονομάζονται Business Email Compromise (BEC), ακριβώς διότι θέτουν σε κίνδυνο το πλέον απαραίτητο εργαλείο επικοινωνίας μιας επιχείρησης.

Ειδικότερα, το Business Email Compromise (BEC) είναι μια εξελιγμένη απάτη που στοχεύει σε επιχειρήσεις και οργανισμούς, στο πλαίσιο της οποίας οι κυβερνοεγκληματίες, είτε χρησιμοποιούν τεχνικές κοινωνικής μηχανικής για να αποκτήσουν πρόσβαση στον λογαριασμό ηλεκτρονικού ταχυδρομείου ενός υπαλλήλου ή ενός στελέχους της εταιρίας, είτε εισβάλλουν αθέμιτα απευθείας στον διακομιστή (server) ηλεκτρονικής της αλληλογραφίας, με σκοπό να αποκτήσουν ελεύθερη πρόσβαση στις θυρίδες του ηλεκτρονικού ταχυδρομείου των υπαλλήλων της, να παραβιάσουν το απόρρητο των επικοινωνιών τους και να λάβουν γνώση όλων των εμπορικών συναλλαγών που πρόκειται να λάβουν χώρα. Στην συνέχεια οι κυβερνοεγκληματίες, έχοντας στην κατοχή τους όλη την ως άνω πληροφορία, δημιουργούν πλαστές θυρίδες ηλεκτρονικού ταχυδρομείου με διευθύνσεις σχεδόν πανομοιότυπες των γνήσιων θυρίδων των υπαλλήλων της επιχείρησης και έτσι υποδυόμενοι εκείνους, παρεμβαίνουν στην επικοινωνία τους με τους πελάτες – προμηθευτές, με σκοπό να τους αποσπάσουν δολίως χρηματικά ποσά.

Όπως καθίσταται αντιληπτό εν αντιθέσει με τις τυπικές απάτες ηλεκτρονικού «ψαρέματος» που μπορεί να στοχεύσουν οποιονδήποτε, τα προγράμματα BEC προσαρμόζονται πολύ προσεκτικά μετά από έρευνα και αναγνώριση των στοιχείων κάθε εταιρείας που τίθεται ως στόχος. Το εν λόγω επίπεδο εξατομίκευσης καθιστά τις επιθέσεις BEC όχι μόνο επιτυχημένες αλλά δύσκολα εντοπίσιμες. Η άμεση δε οικονομική απώλεια σε συνδυασμό με την πιθανή παραβίαση και διαρροή προσωπικών δεδομένων, είναι στοιχεία που μπορεί να πλήξουν κάλλιστα την φήμη και την εμπορική αξιοπιστία μιας επιχείρησης και να της δημιουργήσουν μακροχρόνια ζημία.

3. ΟΡΓΑΝΩΤΙΚΑ ΠΡΟΤΥΠΑ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΩΝ ΚΑΙ ΚΑΝΟΝΙΣΤΙΚΟ ΠΛΑΙΣΙΟ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

3.1 Διασφάλιση της τήρησης των οργανωτικών προτύπων Τεχνολογιών Πληροφορικής και Επικοινωνιών (ΤΠΕ)

Η συμμόρφωση με τα οργανωτικά πρότυπα και τις πολιτικές που διέπουν την Τεχνολογία Πληροφορικής και Επικοινωνιών (ΤΠΕ) συνιστά θεμελιώδη πυλώνα για τη διασφάλιση της κυβερνοασφάλειας, την αποτελεσματική προστασία των πληροφοριακών συστημάτων και τη συνεπή τήρηση των ισχυουσών νομικών και κανονιστικών απαιτήσεων. Στο σύγχρονο ψηφιακό περιβάλλον, όπου οι απειλές στον κυβερνοχώρο εξελίσσονται διαρκώς τόσο σε τεχνικό όσο και σε οργανωτικό επίπεδο, η συμμόρφωση δεν περιορίζεται σε αποσπασματικά τεχνικά μέτρα, αλλά εντάσσεται σε ένα ολοκληρωμένο πλαίσιο διακυβέρνησης της ασφάλειας πληροφοριών.

Στο πλαίσιο αυτό, η διασφάλιση της τήρησης των προτύπων ΤΠΕ προϋποθέτει, κατ' αρχάς, την υιοθέτηση και εφαρμογή συνεκτικών πολιτικών και διαδικασιών ασφάλειας πληροφοριών, εναρμονισμένων με διεθνώς αναγνωρισμένα πρότυπα και κανονιστικά κείμενα, όπως το ISO/IEC 27001, η Οδηγία NIS2 και ο Γενικός Κανονισμός για την Προστασία Δεδομένων (GDPR). Τα πρότυπα αυτά παρέχουν ένα δομημένο και συστηματικό πλαίσιο διαχείρισης κινδύνων, καθορίζοντας σαφείς απαιτήσεις ως προς την προστασία της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των πληροφοριών.

Παράλληλα, ιδιαίτερη σημασία αποδίδεται στην ενσωμάτωση εσωτερικών κανονισμών, διαδικασιών και κανόνων δεοντολογίας στον σχεδιασμό, την ανάπτυξη και τη χρήση των πληροφοριακών υποδομών. Οι κανονιστικές αυτές ρυθμίσεις λειτουργούν συμπληρωματικά προς τα τεχνικά μέτρα ασφαλείας, διαμορφώνοντας ένα σαφές πλαίσιο υπευθυνότητας και ορθής συμπεριφοράς για όλα τα εμπλεκόμενα μέρη. Η αποτελεσματικότητά τους, ωστόσο, εξαρτάται από τον βαθμό κατανόησης και αποδοχής τους από το ανθρώπινο δυναμικό του οργανισμού.

Κεντρικό ρόλο στη διαδικασία συμμόρφωσης διαδραματίζει ο συνεχής έλεγχος εφαρμογής των πολιτικών ασφάλειας μέσω τακτικών εσωτερικών και εξωτερικών ελέγχων (audits), επιθεωρήσεων και επαναξιολογήσεων. Οι μηχανισμοί αυτοί

επιτρέπουν την έγκαιρη ανίχνευση αποκλίσεων, αδυναμιών ή παραλείψεων, συμβάλλοντας στη βελτίωση της συνολικής στάθμης ασφάλειας και στη διαρκή αναπροσαρμογή των οργανωτικών και τεχνικών μέτρων.

Επιπροσθέτως, η εκπαίδευση και η συστηματική ευαισθητοποίηση του προσωπικού αποτελούν κρίσιμη συνιστώσα της συμμόρφωσης με τα πρότυπα ΤΠΕ. Η κατανόηση των υποχρεώσεων που απορρέουν από τις πολιτικές ασφάλειας και το κανονιστικό πλαίσιο ενισχύει την υπεύθυνη χρήση των πληροφοριακών συστημάτων και μειώνει σημαντικά τον κίνδυνο περιστατικών που οφείλονται σε ανθρώπινα σφάλματα ή αμέλεια. Η διάσταση αυτή αποκτά ιδιαίτερη σημασία, δεδομένου ότι ο ανθρώπινος παράγοντας αναγνωρίζεται διεθνώς ως ένας από τους πλέον κρίσιμους παράγοντες κινδύνου στον τομέα της κυβερνοασφάλειας.

Τέλος, η καταγραφή, τεκμηρίωση και ανάλυση αποκλίσεων ή παραβιάσεων των πολιτικών ασφάλειας συνιστά αναγκαία προϋπόθεση για την αποτελεσματική διαχείριση περιστατικών και τη λήψη διορθωτικών και προληπτικών μέτρων. Η τεκμηρίωση αυτή ενισχύει τη διαφάνεια, τη λογοδοσία και τη δυνατότητα απόδειξης συμμόρφωσης έναντι εποπτικών αρχών και λοιπών ενδιαφερόμενων μερών.

Συνεπώς, η συμμόρφωση με τα οργανωτικά πρότυπα δεν αποτελούν, αποκλειστικά τεχνική υποχρέωση, αλλά συνδέονται άρρηκτα με ευρύτερες κοινωνικές, νομικές και ηθικές διαστάσεις, όπως η προστασία της ιδιωτικότητας, η διαφάνεια στη διαχείριση των δεδομένων, η λογοδοσία των οργανισμών απέναντι στους πολίτες και στις αρμόδιες αρχές, καθώς και η αποφυγή διοικητικών και ποινικών κυρώσεων. Ως εκ τούτου, η διασφάλιση της τήρησης των οργανωτικών προτύπων ΤΠΕ αναδεικνύεται σε κρίσιμο παράγοντα θεσμικής αξιοπιστίας, ηθικής συνέπειας και τεχνολογικής ωριμότητας σε κάθε σύγχρονο ψηφιακό οικοσύστημα.

3.2 Οργανωτικό πρότυπο για την ασφάλεια πληροφοριών σε μικρομεσαίες επιχειρήσεις (ΜμΕ)

Η υιοθέτηση οργανωμένων και τυποποιημένων πρακτικών για την ασφάλεια των πληροφοριών αποτελεί βασικό πυλώνα της ψηφιακής ανθεκτικότητας για τις μικρομεσαίες επιχειρήσεις (ΜμΕ). Παρότι οι ΜμΕ συχνά δεν διαθέτουν εξειδικευμένα τμήματα πληροφορικής ή σημαντικούς οικονομικούς πόρους, αποτελούν ιδιαίτερα

ελκυστικό στόχο για κυβερνοεπιθέσεις, λόγω της περιορισμένης ωριμότητας των μηχανισμών ασφάλειας που εφαρμόζουν. Παράλληλα, καλούνται να συμμορφώνονται με αυστηρές νομικές και κανονιστικές απαιτήσεις, όπως ο Γενικός Κανονισμός για την Προστασία Δεδομένων (GDPR), γεγονός που καθιστά αναγκαία την υιοθέτηση ενός συστηματικού πλαισίου διαχείρισης της ασφάλειας πληροφοριών.

Σε αυτό το πλαίσιο, το διεθνές πρότυπο ISO/IEC 27001 για τη Διαχείριση της Ασφάλειας Πληροφοριών (Information Security Management System – ISMS) προσφέρει ένα δομημένο και ευέλικτο πλαίσιο οργανωτικών, τεχνικών και λειτουργικών ελέγχων, το οποίο μπορεί να προσαρμοστεί στο μέγεθος, στη φύση και στις πραγματικές ανάγκες μιας μικρομεσαίας επιχείρησης. Το εν λόγω πρότυπο δεν επιβάλλει ομοιόμορφες λύσεις, αλλά βασίζεται στην αρχή της αναλογικότητας, επιτρέποντας στις ΜμΕ να υιοθετήσουν μέτρα ασφάλειας ανάλογα με το επίπεδο κινδύνου που αντιμετωπίζουν.

Κεντρικός πυρήνας του ISO/IEC 27001 είναι η συστηματική ανάλυση και αξιολόγηση κινδύνων, η οποία προηγείται της επιλογής και εφαρμογής των κατάλληλων ελέγχων ασφάλειας. Η διαδικασία αυτή επιτρέπει στις ΜμΕ να εντοπίζουν τις κρίσιμες πληροφορίες τους, τις απειλές και τις ευπάθειες που τις αφορούν, καθώς και τις πιθανές επιπτώσεις σε περίπτωση παραβίασης. Με βάση τα αποτελέσματα της αποτίμησης κινδύνων, επιλέγονται οι κατάλληλοι έλεγχοι από το Παράρτημα Α (Annex A) του προτύπου, με στόχο τον περιορισμό των κινδύνων σε αποδεκτό επίπεδο.

Ιδιαίτερη σημασία για τις ΜμΕ έχουν τα οργανωτικά μέτρα ασφάλειας, τα οποία περιλαμβάνουν τον σαφή καθορισμό ρόλων και υπευθυνοτήτων για την ασφάλεια των πληροφοριών, την εκπόνηση και έγκριση πολιτικών ασφάλειας από τη διοίκηση, καθώς και τη διαχείριση των σχέσεων με τρίτους παρόχους υπηρεσιών, όπως πάροχοι νεφοϋπολογιστικής. Η ύπαρξη καταγεγραμμένων πολιτικών και η τακτική αναθεώρησή τους, κατόπιν αξιολόγησης κινδύνων, συμβάλλει στη δημιουργία δομής και λογοδοσίας στον τρόπο διαχείρισης των πληροφοριών.

Παράλληλα, το πρότυπο δίνει έμφαση σε τεχνικά και φυσικά μέτρα ασφάλειας, τα οποία είναι άμεσα εφαρμόσιμα στις ΜμΕ. Σε αυτά περιλαμβάνονται ο έλεγχος πρόσβασης στα πληροφοριακά συστήματα, η χρήση ισχυρών μηχανισμών αυθεντικοποίησης, η κρυπτογράφηση ευαίσθητων δεδομένων τόσο κατά την αποθήκευση όσο και κατά τη μεταφορά, καθώς και η ορθή διαχείριση αντιγράφων

ασφαλείας και η περιοδική δοκιμή διαδικασιών αποκατάστασης. Επιπλέον, η προστασία των τελικών συσκευών μέσω λογισμικού antivirus και antimalware, σε συνδυασμό με την έγκαιρη εγκατάσταση ενημερώσεων ασφαλείας, καθώς και η φυσική ασφάλεια του εξοπλισμού, αποτελούν βασικά στοιχεία ενός ελάχιστου αλλά αποτελεσματικού επιπέδου προστασίας.

Καθοριστικό ρόλο στο πλαίσιο του ISO/IEC 27001 διαδραματίζει και ο ανθρώπινος παράγοντας. Η εκπαίδευση και ευαισθητοποίηση του προσωπικού σε θέματα κυβερνοασφάλειας, όπως οι επιθέσεις phishing και οι τεχνικές κοινωνικής μηχανικής, μειώνει σημαντικά την πιθανότητα επιτυχημένων επιθέσεων. Παράλληλα, η θέσπιση κώδικα αποδεκτής χρήσης των πληροφοριακών συστημάτων και πολιτικών για τη χρήση φορητών συσκευών και την απομακρυσμένη εργασία συμβάλλει στη διαμόρφωση κουλτούρας ασφάλειας εντός της επιχείρησης.

Εξίσου σημαντική είναι η πρόβλεψη μηχανισμών διαχείρισης περιστατικών ασφάλειας, οι οποίοι περιλαμβάνουν τη συστηματική καταγραφή περιστατικών, τις διαδικασίες αναφοράς και αντιμετώπισής τους, καθώς και τον σχεδιασμό επιχειρησιακής συνέχειας σε περίπτωση σοβαρής διακοπής λειτουργίας. Η ύπαρξη τέτοιων μηχανισμών επιτρέπει στις ΜμΕ να αντιδρούν έγκαιρα και οργανωμένα σε περιστατικά, περιορίζοντας τις επιπτώσεις τους.

Η υιοθέτηση του ISO/IEC 27001 προσφέρει στις μικρομεσαίες επιχειρήσεις σημαντικά οφέλη, όπως η ενίσχυση της εμπιστοσύνης πελατών και συνεργατών, η βελτίωση της νομικής συμμόρφωσης – ιδίως σε σχέση με τον GDPR – και η δημιουργία ανταγωνιστικού πλεονεκτήματος στην αγορά. Σημαντικό πλεονέκτημα αποτελεί επίσης το γεγονός ότι οι ΜμΕ μπορούν να εφαρμόσουν τις βασικές αρχές και ελέγχους του προτύπου χωρίς να προχωρήσουν άμεσα σε πλήρη πιστοποίηση, υιοθετώντας μια ρεαλιστική και σταδιακή προσέγγιση, η οποία μπορεί να λειτουργήσει ως βάση για μελλοντική πιστοποίηση, εφόσον το απαιτήσουν οι συνθήκες της αγοράς ή οι κανονιστικές εξελίξεις.

3.3 Νομοθετήματα που σχετίζονται με την κυβερνοασφάλεια επιχειρήσεων και οργανισμών

Αυτή η ενότητα εστιάζει στα βασικά κανονιστικά νομοθετήματα που σχετίζονται με την κυβερνοασφάλεια των επιχειρήσεων και των οργανισμών. Εξετάζονται κρίσιμες ρυθμίσεις που αφορούν την προστασία των δεδομένων, την ασφάλεια των δικτύων και πληροφοριών και τη συμμόρφωση των οργανισμών με το θεσμικό πλαίσιο. Μέσω της ανάλυσης αυτών των νομοθετικών και κανονιστικών πλαισίων, αποσαφηνίζεται ο ρόλος της νομικής συμμόρφωσης στην ενίσχυση της κυβερνοανθεκτικότητας, της διαχείρισης κινδύνων και της διασφάλισης της εμπιστοσύνης στις ψηφιακές λειτουργίες των επιχειρήσεων και των οργανισμών.

3.3.1 Ενίσχυση της κυβερνοασφάλειας εντός της Ευρωπαϊκής Ένωσης για επιχειρήσεις και οργανισμούς, σύμφωνα με την οδηγία NIS1 και NIS2

Το πρώτο νομοθέτημα της ΕΕ στον τομέα της κυβερνοασφάλειας είναι η **Οδηγία (ΕΕ) 2016/1148,** ευρέως γνωστή ως NIS1 (από τα αρχικά των λέξεων Network and Information Systems), που εκδόθηκε τον Ιούλιο του 2016, στο πλαίσιο της ευρωπαϊκής στρατηγικής για την ασφάλεια στον κυβερνοχώρο, με στόχο την επίτευξη ενός υψηλού κοινού επιπέδου ασφάλειας για τις κρίσιμες υποδομές σε ολόκληρη την Ευρωπαϊκή Ένωση.

Η NIS1 θεσπίζει υποχρεωτικά μέτρα ασφάλειας και επιχειρησιακής συνέχειας για τα συστήματα δικτύου και πληροφοριών που υποστηρίζουν την παροχή βασικών υπηρεσιών με σημαντικό αντίκτυπο στη σταθερή και εύρυθμη λειτουργία της εσωτερικής αγοράς. Τέτοιες υπηρεσίες περιλαμβάνουν, για παράδειγμα, την προμήθεια ενέργειας σε άτομα και επιχειρήσεις εντός της Ένωσης, αναδεικνύοντας τη σημασία της προστασίας των ψηφιακών υποδομών σε κρίσιμους τομείς για την κοινωνία και την οικονομία.

Σύμφωνα και με τον τίτλο της, η Οδηγία αποσκοπεί στη διαμόρφωση ενός υψηλού και ενιαίου επιπέδου ασφάλειας για τα συστήματα δικτύου και πληροφοριών σε όλα τα κράτη μέλη της Ευρωπαϊκής Ένωσης, με απώτερο στόχο τη βελτιστοποίηση της λειτουργίας της εσωτερικής αγοράς. Στο πλαίσιο αυτό, θεσπίζονται κοινές υποχρεώσεις για την ασφάλεια και την κοινοποίηση περιστατικών, οι οποίες αφορούν τόσο τους φορείς

εκμετάλλευσης βασικών υπηρεσιών όσο και τους παρόχους ψηφιακών υπηρεσιών. Σκοπός των ρυθμίσεων αυτών είναι αφενός η ενίσχυση μιας κουλτούρας πρόληψης και διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας, και αφετέρου η διασφάλιση της έγκαιρης και διαφανούς αναφοράς των σοβαρών περιστατικών ασφάλειας.

Οι βασικοί στόχοι της Οδηγίας επικεντρώνονται στην ενίσχυση της συνολικής ανθεκτικότητας των κρίσιμων υποδομών και των πληροφοριακών συστημάτων της Ευρωπαϊκής Ένωσης έναντι ψηφιακών απειλών. Συγκεκριμένα, επιδιώκεται:

- *η αποτελεσματική διαχείριση των κινδύνων που σχετίζονται με την ασφάλεια των πληροφοριακών συστημάτων,*
- *η προστασία των υποδομών και υπηρεσιών από κυβερνοεπιθέσεις και κακόβουλες ενέργειες,*
- *η έγκαιρη ανίχνευση περιστατικών που σχετίζονται με την κυβερνοασφάλεια, καθώς και*
- *η μείωση των επιπτώσεων που μπορεί να προκαλέσουν τέτοιου είδους περιστατικά στην εύρυθμη λειτουργία κρίσιμων υπηρεσιών και στην κοινωνία γενικότερα.*

Αυτοί οι στόχοι αποτυπώνουν την ανάγκη για μια συνεκτική και στρατηγική προσέγγιση στην αντιμετώπιση των σύγχρονων ψηφιακών απειλών σε επίπεδο Ένωσης. Η Οδηγία εφαρμόζεται άμεσα σε δύο [2] κατηγορίες οργανισμών που δραστηριοποιούνται εντός της Ευρωπαϊκής Ένωσης:

- *Στους Φορείς Εκμετάλλευσης Βασικών Υπηρεσιών (Operators of Essential Services – OES), δηλαδή σε οργανισμούς των οποίων η λειτουργία είναι ζωτικής σημασίας για την κοινωνία και την οικονομία, όπως για παράδειγμα στους τομείς της ενέργειας, των μεταφορών, της υγείας, των τραπεζών και των υποδομών ύδρευσης.*
- *Στους Παρόχους Ψηφιακών Υπηρεσιών (Digital Service Providers – DSP), στους οποίους περιλαμβάνονται επιχειρήσεις που προσφέρουν διαδικτυακές υπηρεσίες, όπως ηλεκτρονικές αγορές (online marketplaces), μηχανές αναζήτησης και υπηρεσίες υπολογιστικού νέφους (cloud computing).*

Η προαναφερόμενη διάκριση αυτή αποσκοπεί στην προσαρμογή των απαιτήσεων ασφάλειας ανάλογα με τη φύση και την κρισιμότητα των παρεχόμενων υπηρεσιών.

Η προαναφερθείσα Οδηγία (ΕΕ) 2016/1148 ενσωματώθηκε στην ελληνική έννομη τάξη με τον Νόμο 4577/2018, ο οποίος ψηφίστηκε τον Δεκέμβριο του 2018. Ο εν λόγω νόμος είναι το πρώτο θεσμικό - νομοθετικό κείμενο για την κυβερνοασφάλεια και καθορίζει το εθνικό πλαίσιο για την ασφάλεια των συστημάτων δικτύου και πληροφοριών, σε συμμόρφωση με τις απαιτήσεις της Οδηγίας NIS. Η Υπουργική Απόφαση 1027/2019 ήρθε να εξειδικεύσει περαιτέρω επιμέρους πτυχές της εφαρμογής του νόμου, ρυθμίζοντας ειδικότερα οργανωτικά και τεχνικά ζητήματα, καθώς και τη λειτουργία των αρμόδιων αρχών.

Εν συνεχεία η Οδηγία (ΕΕ) 2022/2555 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, γνωστή και ως οδηγία NIS2, κατήργησε την προηγούμενη σχετική οδηγία (NIS1) και αποτελεί το νέο νομικό πλαίσιο που αποσκοπεί στην ενίσχυση της κυβερνοασφάλειας εντός της Ευρωπαϊκής Ένωσης. Η εν λόγω οδηγία θεσπίζει διατάξεις που επικεντρώνονται στην ανάπτυξη εθνικής στρατηγικής κυβερνοασφάλειας, στον ορισμό και στην οργάνωση των αρμόδιων αρχών, καθώς και στον συντονισμό των ενεργειών για την αντιμετώπιση κυβερνοκρίσεων και την εποπτεία των κινδύνων στον τομέα αυτόν. Μέσα από την ενίσχυση της συνεργασίας και της κοινής εποπτείας μεταξύ των κρατών μελών, η οδηγία NIS2 στοχεύει στην επίτευξη ενός υψηλού επιπέδου κυβερνοασφάλειας σε ολόκληρη την Ένωση, προστατεύοντας κρίσιμες υποδομές και διασφαλίζοντας τη συνέχεια των υπηρεσιών. Το νέο αυτό θεσμικό πλαίσιο θέτει, μεταξύ άλλων, αυστηρότερες απαιτήσεις για τις επιχειρήσεις, τη δημόσια διοίκηση, τις υποδομές και προβλέπεται να θεσπίσει αυστηρότερες υποχρεώσεις κυβερνοασφάλειας για τη διαχείριση κινδύνων, τις υποχρεώσεις υποβολής εκθέσεων και την ανταλλαγή πληροφοριών. Οι απαιτήσεις καλύπτουν, μεταξύ άλλων διατάξεων, την αντιμετώπιση συμβάντων, την ασφάλεια της αλυσίδας εφοδιασμού, την κρυπτογράφηση και τη δημοσιοποίηση τρωτών σημείων.

Η οδηγία NIS2 εφαρμόζεται σε δημόσιες και ιδιωτικές οντότητες που θεωρούνται μεσαίες επιχειρήσεις, σύμφωνα με τη σύσταση 2003/361/ΕΚ, ή που υπερβαίνουν τα καθορισμένα όρια για τις μεσαίες επιχειρήσεις. Η ενσωμάτωση αυτών των οντοτήτων στο πεδίο εφαρμογής της οδηγίας είναι κρίσιμη, καθώς πολλές από αυτές παρέχουν ζωτικής σημασίας υπηρεσίες ή ασκούν δραστηριότητες που επηρεάζουν την ευρύτερη ασφάλεια και ευημερία της ΕΕ. Με την εφαρμογή της οδηγίας, οι επιχειρήσεις και οι

οργανισμοί καλούνται να υιοθετήσουν ισχυρά μέτρα ασφάλειας, να ενισχύσουν την ανθεκτικότητά τους σε κυβερνοαπειλές και να συμμορφωθούν με αυστηρότερους κανονισμούς που διασφαλίζουν την ασφάλεια των πληροφοριακών τους συστημάτων.

Η οδηγία NIS2 αντιπροσωπεύει μια ουσιαστική εξέλιξη στο πεδίο της κυβερνοασφάλειας για τις επιχειρήσεις και τους οργανισμούς, παρέχοντας ένα σαφές πλαίσιο για την αντιμετώπιση των σύγχρονων απειλών στον κυβερνοχώρο. Η αυξημένη έμφαση στη συνεργασία μεταξύ των κρατών μελών και η ενίσχυση των εθνικών στρατηγικών αναμένεται να βελτιώσουν την προετοιμασία και την απόκριση σε περιστατικά ασφαλείας, προάγοντας ταυτόχρονα την καινοτομία και τη διαφάνεια στις επιχειρηματικές δραστηριότητες. Επομένως, η συμμόρφωση με την οδηγία NIS2 δεν αποτελεί μόνο νομική υποχρέωση, αλλά και μια σημαντική στρατηγική απόφαση για την προστασία των πληροφοριακών υποδομών και τη διασφάλιση της συνεχούς λειτουργίας των οργανισμών στον ψηφιακό κόσμο.

Οντότητες που προστίθενται με την NIS2
Πηγή: https://cyber.gov.gr/

3.3.2 Γενικά μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας σε εφαρμογή της οδηγίας NIS2

Σε εφαρμογή της Οδηγίας (ΕΕ) 2022/2555 (NIS2) και ειδικότερα των διατάξεων του άρθρου 21 και των επόμενων άρθρων αυτής, προβλέπεται ότι οι επιχειρήσεις και οι

οργανισμοί που εμπίπτουν στο πεδίο εφαρμογής της και χαρακτηρίζονται ως υπόχρεες οντότητες υποχρεούνται να λαμβάνουν κατάλληλα και αναλογικά τεχνικά, επιχειρησιακά και οργανωτικά μέτρα για τη διαχείριση των κινδύνων που σχετίζονται με την ασφάλεια των συστημάτων δικτύου και πληροφοριών τα οποία χρησιμοποιούν στο πλαίσιο των δραστηριοτήτων τους ή για την παροχή των υπηρεσιών τους. Σκοπός των μέτρων αυτών είναι η πρόληψη ή, σε κάθε περίπτωση, η ελαχιστοποίηση των επιπτώσεων που δύνανται να προκύψουν από περιστατικά κυβερνοασφάλειας, τόσο για τους αποδέκτες των υπηρεσιών όσο και για άλλες άμεσα ή έμμεσα συνδεδεμένες υπηρεσίες.

Η Οδηγία NIS2 υιοθετεί μια προσέγγιση βασισμένη στον κίνδυνο (risk-based approach), σύμφωνα με την οποία τα μέτρα ασφάλειας οφείλουν να στηρίζονται στα πλέον σύγχρονα τεχνικά δεδομένα και, όπου αυτό είναι εφικτό, στα συναφή ευρωπαϊκά και διεθνή πρότυπα. Παράλληλα, λαμβάνεται ρητά υπόψη το κόστος εφαρμογής των μέτρων, ώστε το επίπεδο προστασίας των συστημάτων δικτύου και πληροφοριών να είναι ανάλογο προς τον υφιστάμενο κίνδυνο. Κατά την αξιολόγηση της αναλογικότητας των μέτρων συνεκτιμώνται παράγοντες όπως ο βαθμός έκθεσης της οντότητας σε απειλές, το μέγεθός της, η πιθανότητα εκδήλωσης περιστατικών και η σοβαρότητα των συνεπειών τους, συμπεριλαμβανομένων των κοινωνικών και οικονομικών επιπτώσεων.

Τα προβλεπόμενα μέτρα διαχείρισης κινδύνων βασίζονται σε μια ολιστική προσέγγιση της κυβερνοασφάλειας, η οποία αποσκοπεί όχι μόνο στην προστασία των ίδιων των συστημάτων δικτύου και πληροφοριών, αλλά και του φυσικού και οργανωτικού περιβάλλοντος εντός του οποίου αυτά λειτουργούν. Η προσέγγιση αυτή περιλαμβάνει ένα ευρύ φάσμα πολιτικών, διαδικασιών και μηχανισμών, οι οποίοι συνθέτουν ένα συνεκτικό πλαίσιο διακυβέρνησης της κυβερνοασφάλειας.

Σε γενικό επίπεδο, η Οδηγία προβλέπει την υιοθέτηση πολιτικών ανάλυσης και διαχείρισης κινδύνων, μηχανισμών χειρισμού περιστατικών κυβερνοασφάλειας, μέτρων επιχειρησιακής συνέχειας και ανάκαμψης από καταστροφές, καθώς και ρυθμίσεων που αφορούν την ασφάλεια της αλυσίδας εφοδιασμού. Επιπλέον, δίνεται έμφαση στην ασφάλεια κατά την απόκτηση, ανάπτυξη και συντήρηση συστημάτων δικτύου και πληροφοριών, στη διαχείριση και γνωστοποίηση ευπαθειών, καθώς και στην τακτική αξιολόγηση της αποτελεσματικότητας των εφαρμοζόμενων μέτρων. Παράλληλα,

αναγνωρίζεται η σημασία βασικών πρακτικών κυβερνοϋγιεινής, της εκπαίδευσης και κατάρτισης του προσωπικού, της χρήσης κρυπτογραφικών μηχανισμών, της ασφάλειας ανθρώπινων πόρων και της υιοθέτησης ισχυρών μηχανισμών ελέγχου πρόσβασης, όπως η πολυπαραγοντική επαλήθευση ταυτότητας.

Τα ανωτέρω μέτρα παρουσιάζονται στην παρούσα ενότητα σε γενικό και συνοπτικό επίπεδο, με σκοπό τη σκιαγράφηση του πλαισίου υποχρεώσεων που εισάγει η Οδηγία NIS2. Η αναλυτική τους εξειδίκευση, τόσο ως προς το περιεχόμενο όσο και ως προς τον τρόπο εφαρμογής τους, εξετάζεται διεξοδικά σε επόμενες υποενότητες της παρούσας εργασίας, όπου αναλύονται ξεχωριστά τα οργανωτικά, τεχνικά και επιχειρησιακά μέτρα κυβερνοασφάλειας.

Η Ελλάδα ενσωμάτωσε την Οδηγία (ΕΕ) 2022/2555 στο εθνικό δίκαιο με τον Νόμο 5160/2024, ο οποίος αποτελεί το νέο θεσμικό πλαίσιο για την ενίσχυση της κυβερνοασφάλειας στη χώρα. Ο νόμος αυτός εκσυγχρονίζει και επεκτείνει το προϋφιστάμενο πλαίσιο του Ν. 4577/2018, εισάγοντας μια περισσότερο ολοκληρωμένη και συστηματική προσέγγιση για την προστασία των κρίσιμων ψηφιακών υποδομών και τη διαχείριση κινδύνων στον κυβερνοχώρο.

Στο επίκεντρο του Ν. 5160/2024 βρίσκεται η διαμόρφωση ενός ενιαίου εθνικού συστήματος διακυβέρνησης της κυβερνοασφάλειας, η καθιέρωση ελάχιστων κοινών οριζόντιων μέτρων διαχείρισης κινδύνων για τις υπόχρεες οντότητες, η ενίσχυση της συνεργασίας και της ανταλλαγής πληροφοριών σε εθνικό και ευρωπαϊκό επίπεδο, καθώς και η θέσπιση μηχανισμών εποπτείας, ελέγχου και επιβολής κυρώσεων. Με τον τρόπο αυτό, το νέο εθνικό πλαίσιο συμβάλλει καθοριστικά στην εναρμόνιση της Ελλάδας με τα σύγχρονα ευρωπαϊκά πρότυπα και στην οικοδόμηση ενός ανθεκτικού και ασφαλούς ψηφιακού περιβάλλοντος.

3.3.3 Λοιπά νομοθετήματα που σχετίζονται με την Κυβερνοασφάλεια

3.3.3.1 Κανονισμός για την ψηφιακή επιχειρησιακή ανθεκτικότητα

Ο Κανονισμός (ΕΕ) 2022/2554, γνωστός και ως DORA (Digital Operational Resilience Act), αποτελεί μια σημαντική εξέλιξη για τις επιχειρήσεις και τους οργανισμούς στον χρηματοοικονομικό τομέα, καθώς στοχεύει στην ενίσχυση της ψηφιακής ανθεκτικότητας

έναντι των κινδύνων που σχετίζονται με τις Τεχνολογίες Πληροφοριών και Επικοινωνιών (ICT). Μέσα από την ενοποίηση και την αναβάθμιση των κανόνων που αφορούν τον κίνδυνο ΤΠΕ, ο κανονισμός DORA δημιουργεί ένα συνεκτικό και ενιαίο πλαίσιο το οποίο εξασφαλίζει ότι όλες οι χρηματοοικονομικές οντότητες θα είναι καλύτερα προετοιμασμένες για να αντιμετωπίσουν σοβαρές επιχειρησιακές διαταραχές.

Η εφαρμογή του κανονισμού DORA θα βοηθήσει τις επιχειρήσεις και τους οργανισμούς να ενισχύσουν τη διαχείριση των κινδύνων ΤΠΕ μέσω της καθιέρωσης μιας ενιαίας προσέγγισης στην αντιμετώπιση αυτών των κινδύνων. Αυτό σημαίνει ότι οι οργανισμοί θα πρέπει να αναπτύξουν ισχυρά μέτρα για την πρόληψη, τον εντοπισμό, την απόκριση και την αποκατάσταση από περιστατικά ΤΠΕ, διασφαλίζοντας έτσι τη συνέχεια των λειτουργιών τους ακόμα και κατά τη διάρκεια κρίσιμων καταστάσεων.

Επιπλέον, ο κανονισμός DORA προωθεί την καλύτερη συνεργασία μεταξύ των επιχειρήσεων και των αρμόδιων αρχών, παρέχοντας ένα σαφές και διαφανές πλαίσιο για την αναφορά και τη διαχείριση περιστατικών ΤΠΕ. Αυτό θα επιτρέψει στους οργανισμούς να ανταλλάσσουν πληροφορίες για τους κινδύνους και τις απειλές που αντιμετωπίζουν, βελτιώνοντας έτσι τη συνολική ασφάλεια του χρηματοοικονομικού τομέα.

Τέλος, η συμμόρφωση με τον Κανονισμό DORA θα ενισχύσει την εμπιστοσύνη των πελατών και των συνεργατών στους οργανισμούς που τον τηρούν, καθώς θα διασφαλίζεται ότι λαμβάνονται τα απαραίτητα μέτρα για την προστασία των δεδομένων και των συστημάτων τους. Με αυτόν τον τρόπο, οι επιχειρήσεις που θα εφαρμόσουν τις διατάξεις του κανονισμού θα μπορούν να αποκτήσουν ανταγωνιστικό πλεονέκτημα, προσφέροντας ασφαλέστερες και πιο αξιόπιστες υπηρεσίες στους πελάτες τους.

3.3.4 Ο Κανονισμός για την Τεχνητή Νοημοσύνη και η επίδρασή του σε επιχειρήσεις και οργανισμούς

Η Πράξη για την Τεχνητή Νοημοσύνη (AI Act) της Ευρωπαϊκής Ένωσης [Κανονισμός (ΕΕ) 2024/1689(ΕΕ), γνωστός και ως Κανονισμός για την Τεχνητή Νοημοσύνη] αποτελεί ένα πρωτοποριακό νομικό πλαίσιο που στοχεύει στη ρύθμιση της χρήσης τεχνολογιών Τεχνητής Νοημοσύνης (AI) σε ολόκληρη την Ευρώπη. Η νέα αυτή νομοθεσία θα έχει σημαντική επίδραση στις επιχειρήσεις και στους οργανισμούς,

εισάγοντας αυστηρούς κανόνες για τη χρήση, την ανάπτυξη και τη διάθεση των συστημάτων AI. Με την AI Act, οι επιχειρήσεις καλούνται να διασφαλίσουν ότι οι τεχνολογίες τεχνητής νοημοσύνης που χρησιμοποιούν συμμορφώνονται με συγκεκριμένα πρότυπα ασφάλειας, διαφάνειας και λογοδοσίας, μειώνοντας έτσι τους κινδύνους που σχετίζονται με την κακή χρήση της AI.

Η συμμόρφωση με την AI Act θα απαιτήσει από τις επιχειρήσεις να αναθεωρήσουν και να προσαρμόσουν τις διαδικασίες ανάπτυξης και διάθεσης των συστημάτων AI που χρησιμοποιούν. Για πολλές εταιρείες, αυτό μπορεί να συνεπάγεται αυξημένα κόστη για τη διασφάλιση της συμμόρφωσης, καθώς και την ανάγκη για επιπλέον εκπαίδευση του προσωπικού τους σχετικά με τις νέες ρυθμίσεις. Ταυτόχρονα, η πράξη θα ενθαρρύνει την καινοτομία, προσφέροντας ένα σαφές και σταθερό πλαίσιο λειτουργίας για τις επιχειρήσεις που επενδύουν σε τεχνολογίες AI, δίνοντάς τους τη δυνατότητα να αξιοποιήσουν πλήρως τις δυνατότητες της τεχνητής νοημοσύνης με ασφαλή και υπεύθυνο τρόπο.

Τέλος, η AI Act θα συμβάλλει στην ενίσχυση της εμπιστοσύνης των καταναλωτών και των συνεργατών προς τις τεχνολογίες AI, προσφέροντας μια εγγύηση ότι τα συστήματα AI που χρησιμοποιούνται από τις επιχειρήσεις πληρούν υψηλά πρότυπα ηθικής και διαφάνειας. Αυτό θα μπορούσε να αποτελέσει ένα σημαντικό ανταγωνιστικό πλεονέκτημα για τις εταιρείες που συμμορφώνονται με τις νέες απαιτήσεις, να βελτιώσει τη φήμη τους και να προσελκύσει περισσότερους πελάτες που αναζητούν υπεύθυνες και ασφαλείς τεχνολογικές λύσεις.

3.3.5 Θεσμικό πλαίσιο προστασίας προσωπικών δεδομένων επιχειρήσεων και οργανισμών

Το σημαντικότερο νομοθέτημα στον τομέα της προστασίας προσωπικών δεδομένων είναι ο Γενικός Κανονισμός Προστασίας Δεδομένων (ΓΚΠΔ) (ΕΕ 679/2016), η έναρξη ισχύος του οποίου πραγματοποιήθηκε στις 25 Μαΐου 2018 και ο οποίος μετέβαλε έκτοτε οριστικά το τοπίο στην παγκόσμια «ψηφιακή» οικονομία σε επιχειρήσεις και οργανισμούς εντός αλλά και εκτός των ορίων της Ευρωπαϊκής Ένωσης.

Ο Γενικός Κανονισμός Προστασίας Δεδομένων (General Data Protection Regulation, γνωστός και ως GDPR) είναι ένα καινοτόμο νομοθέτημα που επιδιώκει την ενδυνάμωση των ατομικών δικαιωμάτων των υποκειμένων των δεδομένων, δηλαδή των Ευρωπαίων πολιτών ή ορθότερα των φυσικών προσώπων που διαμένουν μόνιμα εντός της Ευρωπαϊκής Ένωσης (European residents), και δημιουργεί ένα σαφές και αυστηρό πλαίσιο επεξεργασίας των προσωπικών δεδομένων σε μια επιχείρηση.

Η μεταρρύθμιση και η αναβάθμιση της προστασίας των δεδομένων αποτελεί νομοθετική δέσμη με σκοπό την επικαιροποίηση και τον εκσυγχρονισμό των υφιστάμενων κανόνων. Περιλαμβάνει δύο νομοθετικές πράξεις:

1. τον Γενικό Κανονισμό Προστασίας Δεδομένων (που αντικαθιστά την οδηγία 95/46/ΕΚ), και
2. την Οδηγία (ΕΕ) 2016/680.

Ο νέος Γενικός Κανονισμός Προστασίας Δεδομένων περιγράφει τον τρόπο αναγνώρισης και προστασίας των δεδομένων προσωπικού χαρακτήρα, ενώ παρέχει τους βασικούς ορισμούς, ώστε να μπορέσουμε αρχικά να αναγνωρίσουμε ποια δεδομένα είναι δεδομένα προσωπικού χαρακτήρα, δηλαδή κάθε πληροφορία που αφορά φυσικό πρόσωπο, με βάση την οποία αυτό ταυτοποιείται ή/και αναγνωρίζεται. Υπάρχουν δύο κατηγορίες δεδομένων, τα απλά και τα ειδικής κατηγορίας/ευαίσθητα.

Επιπλέον, ο κανονισμός καθορίζει σε ποιες περιπτώσεις επιτρέπεται τα δεδομένα να χρησιμοποιούνται, να αποθηκεύονται, να διαγράφονται, να μεταβιβάζονται και εν γένει να τυγχάνουν επεξεργασίας. Επίσης, καθορίζει τον τρόπο προστασίας και ενημέρωσης του υποκειμένου των δεδομένων, τις αρμόδιες αρχές για την επίβλεψη της εφαρμογής του αλλά και τις κυρώσεις σε περιπτώσεις παραβιάσεων. Η εν λόγω κανονισμός αλλά και η Οδηγία (ΕΕ) 2016/680 ενσωματώθηκε στο εθνικό μας δίκαιο με τον εφαρμοστικό Νόμο 4624/2019.

4. ΑΡΜΟΔΙΕΣ ΑΡΧΕΣ ΓΙΑ ΤΗΝ ΕΠΙΒΟΛΗ ΚΑΙ ΤΗΝ ΕΦΑΡΜΟΓΗ ΤΗΣ ΝΟΜΟΘΕΣΙΑΣ ΓΙΑ ΤΗΝ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ ΣΤΗΝ ΧΩΡΑ ΜΑΣ

4.1 Εθνική Αρχή Κυβερνοασφάλειας (ΕΑΚ)

4.1.1 Σύσταση και σκοπός της Εθνικής Αρχής Κυβερνοασφάλειας (ΕΑΚ)

Με τον ν. 5086/2024 συστάθηκε η Εθνική Αρχή Κυβερνοασφάλειας (ΕΑΚ) **ως** νομικό πρόσωπο δημοσίου δικαίου (Ν.Π.Δ.Δ.), με έδρα την Αθήνα και εποπτεία από τον Υπουργό Ψηφιακής Διακυβέρνησης. Στις διεθνείς της σχέσεις φέρει την επωνυμία National Cybersecurity Authority (NCSA). Η ένταξή της στον δημόσιο τομέα και η απονομή σε αυτήν όλων των διοικητικών, οικονομικών και δικαστικών ατελειών, καθώς και των δικονομικών και ουσιαστικών προνομίων του Δημοσίου, καταδεικνύουν τον ρόλο της ως κεντρικού θεσμικού φορέα άσκησης δημόσιας πολιτικής στον τομέα της κυβερνοασφάλειας.

Αποστολή και σκοπός της Εθνικής Αρχής Κυβερνοασφάλειας είναι η οργάνωση, ο συντονισμός, η εφαρμογή και ο έλεγχος ενός ολοκληρωμένου πλαισίου στρατηγικών, μέτρων και δράσεων με στόχο την επίτευξη υψηλού επιπέδου κυβερνοασφάλειας σε εθνικό επίπεδο. Ο σκοπός αυτός εκτείνεται σε όλο το φάσμα της διαχείρισης κυβερνοκινδύνων, περιλαμβάνοντας την πρόληψη, την προστασία και την αποτροπή κυβερνοαπειλών, καθώς και τον εντοπισμό, την αντιμετώπιση, την αποκατάσταση και την ανάκαμψη από κυβερνοεπιθέσεις.

Για την υλοποίηση του σκοπού της, η ΕΑΚ χαράσσει την ενιαία πολιτική κυβερνοασφάλειας στο πλαίσιο της Στρατηγικής Εθνικής Ασφάλειας, όπως αυτή διαμορφώνεται από τα αρμόδια κυβερνητικά όργανα. Παράλληλα, έχει την αρμοδιότητα διαμόρφωσης, σύνταξης και επικαιροποίησης της Εθνικής Στρατηγικής Κυβερνοασφάλειας, καθώς και του συντονισμού, της εποπτείας και της αξιολόγησης της εφαρμογής της, μέσω της υποβολής σχετικών αναφορών προς τον Υπουργό Ψηφιακής Διακυβέρνησης και την αρμόδια Επιτροπή Συντονισμού για θέματα Κυβερνοασφάλειας.

Η Αρχή συμβάλλει ενεργά στη διαμόρφωση του κανονιστικού πλαισίου κυβερνοασφάλειας, εισηγούμενη την υιοθέτηση νομοθετικών μέτρων και την έκδοση κανονιστικών πράξεων, ενώ ταυτόχρονα ενισχύει τον θεσμικό συντονισμό μεταξύ των αρμόδιων φορέων. Επιπλέον, αναπτύσσει και προτείνει πλαίσια κινήτρων για επενδύσεις

στον τομέα της κυβερνοασφάλειας, σε συνεργασία με συναρμόδια υπουργεία και εποπτευόμενους φορείς, και συμμετέχει στη διαχείριση της εθνικής κοινότητας κυβερνοασφάλειας στο πλαίσιο της ενωσιακής αρχιτεκτονικής συντονισμού.

Ιδιαίτερη έμφαση αποδίδεται από την ΕΑΚ στην εκπαίδευση, την ενημέρωση και την ευαισθητοποίηση σε θέματα κυβερνοασφάλειας, καθώς και στην ενίσχυση της επιστημονικής έρευνας και της ανάπτυξης καινοτόμων υπηρεσιών, εφαρμογών και τεχνολογικών λύσεων. Παράλληλα, προωθείται η συνεργασία με δημόσιους, ιδιωτικούς, ακαδημαϊκούς και ερευνητικούς φορείς, με στόχο τη συγκρότηση ενός συνεκτικού εθνικού οικοσυστήματος κυβερνοασφάλειας.

Στο επιχειρησιακό επίπεδο, η ΕΑΚ διαμορφώνει και παρακολουθεί το πλαίσιο τεχνικών μέτρων και απαιτήσεων ασφάλειας των συστημάτων Τεχνολογιών Πληροφορικής και Επικοινωνιών και λαμβάνει τεχνικά μέτρα αποτροπής και αντιμετώπισης κυβερνοαπειλών, σε συνεργασία με τις κατά περίπτωση αρμόδιες αρχές, και ιδίως με την Ελληνική Αστυνομία. Περαιτέρω, ασκεί ελεγκτικές αρμοδιότητες, διενεργεί επιθεωρήσεις και επιβάλλει κυρώσεις στο πλαίσιο του ελέγχου συμμόρφωσης προς το ισχύον νομικό πλαίσιο κυβερνοασφάλειας.

Η Αρχή αναπτύσσει και υλοποιεί πλαίσιο πιστοποίησης κυβερνοασφάλειας για προϊόντα, διαδικασίες, υπηρεσίες και παρόχους, σύμφωνα με τα ευρωπαϊκά σχήματα πιστοποίησης, ενώ παράλληλα παρακολουθεί το συνολικό επίπεδο ασφάλειας του κυβερνοχώρου στη χώρα. Σημαντικός είναι, επίσης, ο ρόλος της στη διαχείριση κυβερνοπεριστατικών και κρίσεων, μέσω της λειτουργίας του Ενοποιημένου Κέντρου Επιχειρήσεων Ασφάλειας (ΕΚΕΑ), του Εθνικού Δικτύου SOC και της Ομάδας Απόκρισης Συμβάντων στον Κυβερνοχώρο (CSIRT).

Η Εθνική Αρχή Κυβερνοασφάλειας λειτουργεί ως το ενιαίο εθνικό σημείο αναφοράς για απειλές και συμβάντα στον κυβερνοχώρο, συλλέγοντας, αναλύοντας και διαμοιράζοντας πληροφορίες σε συνεργασία με δημόσιους και ιδιωτικούς φορείς, καθώς και με αρμόδιες αρχές σε εθνικό, ενωσιακό και διεθνές επίπεδο. Παράλληλα, παρέχει κατευθυντήριες γραμμές και δεσμευτικές οδηγίες προς δημόσιους και ιδιωτικούς φορείς και ενημερώνει, χωρίς καθυστέρηση, τα αρμόδια όργανα σε περιπτώσεις εξαιρετικών κυβερνοσυμβάντων που ενέχουν στρατηγικό κίνδυνο.

Τέλος, η άσκηση του σκοπού και των αρμοδιοτήτων της Αρχής λαμβάνει χώρα με γνώμονα την προστασία των ουσιωδών συμφερόντων της εθνικής ασφάλειας, της άμυνας και της δημόσιας τάξης και ασφάλειας, καθώς και την προάσπιση των ατομικών δικαιωμάτων στον κυβερνοχώρο. Στο πλαίσιο αυτό, η ΕΑΚ συνεργάζεται με τις αρμόδιες υπηρεσίες του Υπουργείου Εθνικής Άμυνας, του Υπουργείου Προστασίας του Πολίτη και την Εθνική Υπηρεσία Πληροφοριών, χωρίς να επεκτείνει τις αρμοδιότητές της σε συστήματα και δίκτυα που υπάγονται σε ειδικούς κανόνες προστασίας διαβαθμισμένων πληροφοριών.

4.1.2 Οργάνωση και διοικητική διάρθρωση της Εθνικής Αρχής Κυβερνοασφάλειας

Η Εθνική Αρχή Κυβερνοασφάλειας συγκροτείται και λειτουργεί βάσει συγκεκριμένης οργανωτικής και διοικητικής διάρθρωσης, η οποία αποσκοπεί στη διακριτή κατανομή επιτελικών, στρατηγικών, ρυθμιστικών και επιχειρησιακών αρμοδιοτήτων, υπό την ενιαία διοίκηση και εποπτεία του Διοικητή της Αρχής.

Σε κεντρικό επίπεδο, η Αρχή διαρθρώνεται σε οργανικές μονάδες που υπάγονται απευθείας στον Διοικητή και περιλαμβάνουν, καταρχάς, το Γραφείο Διοικητή, το οποίο υποστηρίζει τη διοίκηση της Αρχής και τη συνολική άσκηση των αρμοδιοτήτων της.

Περαιτέρω, στην οργανωτική δομή της Αρχής εντάσσονται δύο βασικές Γενικές Διευθύνσεις με διακριτό αντικείμενο. Η Γενική Διεύθυνση Επιτελικού Σχεδιασμού συγκεντρώνει τις οργανικές μονάδες που ασκούν αρμοδιότητες επιτελικού, στρατηγικού και ρυθμιστικού χαρακτήρα. Στο πλαίσιο αυτό, η εν λόγω Γενική Διεύθυνση είναι αρμόδια, μεταξύ άλλων, για τον σχεδιασμό και την εποπτεία της συμμόρφωσης προς το κανονιστικό πλαίσιο της κυβερνοασφάλειας, τον προγραμματισμό ελέγχων και επιθεωρήσεων, τον επενδυτικό σχεδιασμό που αφορά στις αρμοδιότητες της Αρχής ως Εθνικού Κέντρου Συντονισμού, τον καθορισμό προτεραιοτήτων στους τομείς της έρευνας και της καινοτομίας, καθώς και για την προαγωγή των διεθνών συνεργασιών στον χώρο της κυβερνοασφάλειας. Παράλληλα, υπάγονται σε αυτήν αρμοδιότητες που σχετίζονται με την ενημέρωση, την εκπαίδευση και την ευαισθητοποίηση δημόσιων και ιδιωτικών φορέων.

Η Γενική Διεύθυνση Επιχειρησιακού Σχεδιασμού αποτελεί τον πυρήνα των επιχειρησιακών και τεχνικών λειτουργιών της Αρχής. Σε αυτήν υπάγονται οι οργανικές μονάδες που είναι επιφορτισμένες με την εποπτεία του κυβερνοχώρου, την πρόληψη, την προστασία και την αντιμετώπιση κυβερνοαπειλών, καθώς και με τη διασφάλιση της επιχειρησιακής συνέχειας κρίσιμων λειτουργιών. Επιπλέον, η εν λόγω Γενική Διεύθυνση έχει την ευθύνη της διεξαγωγής των ελέγχων και επιθεωρήσεων, της διαχείρισης περιστατικών στον κυβερνοχώρο και της λειτουργίας των βασικών επιχειρησιακών δομών της Αρχής.

Στο πλαίσιο αυτό, στην Εθνική Αρχή Κυβερνοασφάλειας λειτουργούν το Κέντρο Επιχειρήσεων Κυβερνοασφάλειας (Security Operations Centre – SOC), η Ομάδα Απόκρισης Συμβάντων στον Κυβερνοχώρο (CSIRT), καθώς και το Εργαστήριο Αναλύσεων, Δοκιμών και Ερευνών (Forensics & Testing Lab). Οι δομές αυτές αποτελούν κρίσιμους μηχανισμούς για την παρακολούθηση του κυβερνοχώρου, την ανάλυση και αξιολόγηση απειλών, την τεχνική διερεύνηση περιστατικών και την επιχειρησιακή απόκριση σε κυβερνοεπιθέσεις.

Προς διασφάλιση της χρηστής διοίκησης, της διαφάνειας και της αποτελεσματικής λειτουργίας της, στην Αρχή συστήνεται Μονάδα Εσωτερικού Ελέγχου, η οποία λειτουργεί σε επίπεδο Τμήματος και υπάγεται απευθείας στον Διοικητή. Η Μονάδα Εσωτερικού Ελέγχου ασκεί τους επιχειρησιακούς στόχους και τις αρμοδιότητες που προβλέπονται στο άρθρο 10 του ν. 4795/2021, συμβάλλοντας στον έλεγχο της νομιμότητας, της κανονικότητας και της αποδοτικότητας της διοικητικής και επιχειρησιακής δράσης της Εθνικής Αρχής Κυβερνοασφάλειας.

4.1.3 Εθνική Αρχή Αντιμετώπισης Ηλεκτρονικών Επιθέσεων - Εθνικό CERT

Η Εθνική Αρχή Αντιμετώπισης Ηλεκτρονικών Επιθέσεων – Εθνικό CERT συνιστά τον κεντρικό εθνικό μηχανισμό πρόληψης, έγκαιρης προειδοποίησης και αντιμετώπισης κυβερνοεπιθέσεων που στρέφονται κατά των πληροφοριακών συστημάτων του δημόσιου τομέα και των κρίσιμων υποδομών της χώρας. Η αποστολή της εδράζεται στην ανάγκη διασφάλισης της λειτουργικής συνέχειας των δημόσιων οργανισμών, της προστασίας των πληροφοριακών πόρων και, κατ' επέκταση, της εθνικής ασφάλειας στον

κυβερνοχώρο, σε ένα περιβάλλον αυξανόμενων, σύνθετων και συχνά διασυνοριακών κυβερνοαπειλών.

Το θεσμικό πλαίσιο λειτουργίας της Αρχής καθορίζεται πρωτίστως από το Π.Δ. 1/2017, όπως αυτό τροποποιήθηκε με τα Π.Δ. 96/2020 και 33/2022, τα οποία προσδιορίζουν την κοινότητα αρμοδιότητάς της και τον ρόλο της ως Ομάδας Αντιμετώπισης Ηλεκτρονικών Επιθέσεων (National CERT). Σύμφωνα με τις διατάξεις αυτές, η κοινότητα αποδεκτών της περιλαμβάνει κατά προτεραιότητα την Προεδρία της Κυβέρνησης, τα Υπουργεία και τους εποπτευόμενους φορείς τους, καθώς και τον ευρύτερο δημόσιο τομέα, με εξαίρεση τους φορείς που υπάγονται στην αρμοδιότητα της Διεύθυνσης Κυβερνοάμυνας του Γενικού Επιτελείου Εθνικής Άμυνας. Ο σαφής αυτός καταμερισμός αρμοδιοτήτων διασφαλίζει τη διάκριση μεταξύ πολιτικής κυβερνοασφάλειας και στρατιωτικής κυβερνοάμυνας, ενισχύοντας την επιχειρησιακή αποτελεσματικότητα του εθνικού πλαισίου κυβερνοπροστασίας.

Η Εθνική Αρχή Αντιμετώπισης Ηλεκτρονικών Επιθέσεων υπάγεται οργανωτικά στη Διεύθυνση Κυβερνοχώρου της Εθνικής Υπηρεσίας Πληροφοριών (ΕΥΠ), γεγονός που αναδεικνύει τον στρατηγικό χαρακτήρα της κυβερνοασφάλειας ως ζητήματος εθνικής σημασίας. Στο πλαίσιο αυτό, η ΕΥΠ ασκεί τις αρμοδιότητες της Εθνικής Αρχής, όπως αυτές προβλέπονται στο άρθρο 4 παρ. 8 του ν. 3649/2008 και στο Π.Δ. 325/2003, με έμφαση τόσο στη στατική όσο και στην ενεργητική αντιμετώπιση ηλεκτρονικών επιθέσεων κατά δικτύων επικοινωνιών, συστημάτων πληροφορικής και υποδομών αποθήκευσης πληροφοριών.

Σε επιχειρησιακό επίπεδο, το Εθνικό CERT διαδραματίζει καθοριστικό ρόλο στη διαχείριση κυβερνοπεριστατικών, καλύπτοντας όλο τον κύκλο ζωής τους, από την αρχική ανίχνευση και αξιολόγηση έως την αποκατάσταση και την πρόληψη επανάληψης. Η Αρχή συλλέγει, διατηρεί και αναλύει ψηφιακά πειστήρια που σχετίζονται με ηλεκτρονικές επιθέσεις και απειλές, υποστηρίζοντας δημόσιους οργανισμούς και κρίσιμες υποδομές στην τεχνική και οργανωτική διαχείριση των περιστατικών. Παράλληλα, αναλύει και κατηγοριοποιεί τους τύπους των κυβερνοεπιθέσεων, προσαρμόζοντας τις ενέργειες αντιμετώπισης ανάλογα με τη φύση, την ένταση και τις επιπτώσεις τους.

Ιδιαίτερη σημασία αποδίδεται στη λειτουργία της αντίδρασης σε περιστατικά, στο πλαίσιο της οποίας το Εθνικό CERT προβαίνει στη διακρίβωση της πραγματικής ύπαρξης ενός περιστατικού ασφαλείας, στην εκτίμηση των επιπτώσεών του και στον συντονισμό των εμπλεκόμενων φορέων. Οι ενέργειες αυτές περιλαμβάνουν, μεταξύ άλλων, τον εντοπισμό της αρχικής αιτίας του περιστατικού, τη διευκόλυνση της επικοινωνίας με διωκτικές αρχές όπου απαιτείται, τη σύνταξη και ανταλλαγή αναφορών με άλλα CERTs και CSIRTs, καθώς και τον συντονισμό της απόκρισης σε κατανεμημένες επιθέσεις μεγάλης κλίμακας. Παρά την υποστήριξη που παρέχεται, η ευθύνη για την ασφαλή λειτουργία των πληροφοριακών συστημάτων και την τελική επίλυση των περιστατικών παραμένει στους ίδιους τους ιδιοκτήτες των συστημάτων, στοιχείο που συνάδει με τις αρχές της διοικητικής αυτοτέλειας και της λογοδοσίας των δημόσιων οργανισμών.

Παράλληλα με την αντιμετώπιση περιστατικών, το Εθνικό CERT αναπτύσσει εκτεταμένες δράσεις πρόληψης, οι οποίες αποσκοπούν στη μείωση της επιφάνειας επίθεσης και στην ενίσχυση της κυβερνοανθεκτικότητας του δημόσιου τομέα. Στο πλαίσιο αυτό, εκδίδει προειδοποιήσεις και ανακοινώσεις για αναδυόμενες απειλές, προτείνει μέτρα και εργαλεία ασφάλειας, παράγει κανόνες και έγγραφα βέλτιστων πρακτικών και διενεργεί αξιολογήσεις τρωτοτήτων κατόπιν αιτήματος των φορέων. Επιπλέον, η εκπαίδευση των στελεχών πληροφορικής των κυβερνητικών οργανισμών αποτελεί βασικό πυλώνα της προληπτικής στρατηγικής, συμβάλλοντας στη διαμόρφωση κουλτούρας κυβερνοασφάλειας εντός της δημόσιας διοίκησης.

Η αποτελεσματική λειτουργία της Εθνικής Αρχής Αντιμετώπισης Ηλεκτρονικών Επιθέσεων ενισχύεται σημαντικά μέσω της συνεργασίας και της διαλειτουργικότητας με άλλες εθνικές και διεθνείς αρχές και φορείς. Η Αρχή συνεργάζεται με άλλα CSIRT, με υπηρεσίες του δημόσιου τομέα, καθώς και με αρμόδιους εθνικούς και διεθνείς οργανισμούς κυβερνοασφάλειας. Ειδικότερα, για ζητήματα εθνικής σημασίας συνεργάζεται με την Κυβέρνηση και την Εθνική Αρχή Κυβερνοασφάλειας του Υπουργείου Ψηφιακής Διακυβέρνησης, για θέματα προστασίας δεδομένων με την Αρχή Προστασίας Προσωπικών Δεδομένων, ενώ για ύποπτη εγκληματική δραστηριότητα συνεργάζεται με τη Διεύθυνση Δίωξης Κυβερνοεγκλήματος της Ελληνικής Αστυνομίας. Η συνεργασία αυτή επιτρέπει τον αποτελεσματικό συντονισμό δράσεων σε κρίσιμες

καταστάσεις και την εφαρμογή της εθνικής στρατηγικής κυβερνοασφάλειας σε εθνικό και διεθνές επίπεδο.

Ιδιαίτερη βαρύτητα αποδίδεται στην προστασία των πληροφοριών και των δεδομένων που διαχειρίζεται η Αρχή. Η αποκάλυψη πληροφοριών πραγματοποιείται αποκλειστικά στο πλαίσιο της αρχής της «ανάγκης γνώσης» και κατόπιν εξουσιοδότησης του ιδιοκτήτη της πληροφορίας, διασφαλίζοντας την εμπιστευτικότητα και την ακεραιότητα τόσο εταιρικών όσο και ιδιωτικών δεδομένων.

Η λειτουργία και οι αρμοδιότητες της Εθνικής Αρχής Αντιμετώπισης Ηλεκτρονικών Επιθέσεων αποκτούν ιδιαίτερη σημασία υπό το πρίσμα της Οδηγίας (ΕΕ) 2022/2555 (NIS 2), η οποία εισάγει αυξημένες απαιτήσεις για την ασφάλεια δικτύων και πληροφοριακών συστημάτων, ενισχύοντας τον ρόλο των εθνικών CSIRT και των αρμόδιων αρχών. Η NIS 2 δίνει έμφαση στην πρόληψη, στην έγκαιρη κοινοποίηση περιστατικών, στον συντονισμό σε εθνικό και ευρωπαϊκό επίπεδο και στην ενίσχυση της ανθεκτικότητας κρίσιμων και σημαντικών οντοτήτων. Στο πλαίσιο αυτό, το Εθνικό CERT καλείται να διαδραματίσει ενισχυμένο ρόλο ως κόμβος τεχνικής υποστήριξης, συντονισμού και ανταλλαγής πληροφοριών, συμβάλλοντας ουσιαστικά στην εφαρμογή των νέων απαιτήσεων της Οδηγίας και στη συνολική αναβάθμιση της κυβερνοασφάλειας του δημόσιου τομέα στην Ελλάδα.

5. Ο ΡΟΛΟΣ ΤΟΥ ΥΠΕΥΘΥΝΟΥ ΑΣΦΑΛΕΙΑΣ ΣΥΣΤΗΜΑΤΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ (Υ.Α.Σ.Π.Ε.) ΣΤΟ ΠΛΑΙΣΙΟ ΣΥΜΜΟΡΦΩΣΗΣ ΜΕ ΤΗΝ ΟΔΗΓΙΑ NIS2 ΚΑΙ ΤΟΝ Ν. 5160/2024

5.1 Θεσμικό πλαίσιο και νομική θεμελίωση του ρόλου του Υ.Α.Σ.Π.Ε.

Ο Υπεύθυνος Ασφάλειας Συστημάτων Πληροφορικής και Επικοινωνιών (Υ.Α.Σ.Π.Ε.), ο οποίος στην πράξη ταυτίζεται λειτουργικά με τον ρόλο του Chief Information Security Officer (CISO), αναδεικνύεται σε κομβικό θεσμικό και επιχειρησιακό παράγοντα εφαρμογής της Οδηγίας (ΕΕ) 2022/2555 (NIS 2) στο εθνικό δίκαιο. Με τον ν. 5160/2024 και τις συναφείς κανονιστικές πράξεις, ο ρόλος του Υ.Α.Σ.Π.Ε. αποκτά σαφή

νομική θεμελίωση, διευρυμένες αρμοδιότητες και αυξημένες απαιτήσεις ανεξαρτησίας, αντανακλώντας τη μετατόπιση της κυβερνοασφάλειας από τεχνικό ζήτημα σε ζήτημα στρατηγικής διακυβέρνησης και διοικητικής ευθύνης.

Σύμφωνα με το άρθρο 15 του ν. 5160/2024, οι βασικές και οι σημαντικές οντότητες υποχρεούνται να ορίζουν στέλεχος κατάλληλων προσόντων και εμπειρογνωμοσύνης ως Υ.Α.Σ.Π.Ε., ο οποίος λειτουργεί ως το κεντρικό σημείο επαφής της οντότητας με την Εθνική Αρχή Κυβερνοασφάλειας. Ο ρόλος αυτός δεν περιορίζεται στην εξωτερική επικοινωνία, αλλά επεκτείνεται στην εσωτερική επιμέλεια και στον συντονισμό όλων των ενεργειών που απαιτούνται για τη συμμόρφωση της οντότητας με τις υποχρεώσεις διαχείρισης κινδύνων και αναφοράς περιστατικών κυβερνοασφάλειας. Η θεσμική πρόβλεψη του Υ.Α.Σ.Π.Ε. αποτυπώνει με σαφήνεια την απαίτηση της NIS 2 για ορισμό υπευθύνου με πραγματική επιχειρησιακή αρμοδιότητα και όχι απλώς τυπικό ή συμβουλευτικό ρόλο.

Ιδιαίτερη σημασία αποδίδεται στην αυτονομία και τη θέση του Υ.Α.Σ.Π.Ε. εντός της οργανωτικής δομής. Ο νομοθέτης απαιτεί ο Υ.Α.Σ.Π.Ε. να διαθέτει κατάλληλο και επαρκές επίπεδο αυτονομίας στη λήψη αποφάσεων, δυνατότητα εφαρμογής τους από τις επιμέρους οργανικές μονάδες, καθώς και άμεση πρόσβαση και λογοδοσία στο ανώτατο διοικητικό επίπεδο της οντότητας. Η πρόβλεψη αυτή συνδέεται άμεσα με τη φιλοσοφία της NIS 2, η οποία καθιστά τα όργανα διοίκησης συνυπεύθυνα για την κυβερνοασφάλεια και απαιτεί τη συστηματική ενημέρωσή τους σχετικά με τους υφιστάμενους κινδύνους και τις κυβερνοαπειλές.

5.2 Καθήκοντα και αρμοδιότητες του Υ.Α.Σ.Π.Ε.

Τα καθήκοντα του Υ.Α.Σ.Π.Ε. είναι πολυεπίπεδα και καλύπτουν τόσο τον στρατηγικό όσο και τον επιχειρησιακό τομέα της κυβερνοασφάλειας. Μεταξύ αυτών περιλαμβάνεται η διαρκής μέριμνα για την ασφάλεια των συστημάτων δικτύου και πληροφοριών της οντότητας, η εποπτεία της υλοποίησης των τεχνικών και οργανωτικών μέτρων κυβερνοασφάλειας, καθώς και ο συντονισμός της διαχείρισης περιστατικών ασφαλείας. Παράλληλα, ο Υ.Α.Σ.Π.Ε. επιμελείται τη συμμόρφωση της οντότητας με τις απαιτήσεις κοινοποίησης σημαντικών περιστατικών και εθελούσιας αναφοράς

κυβερνοαπειλών προς την αρμόδια ομάδα απόκρισης (CSIRT), διασφαλίζοντας την έγκαιρη και ορθή ροή πληροφοριών, όπως επιτάσσει η NIS 2.

Κεντρικό στοιχείο του ρόλου του Υ.Α.Σ.Π.Ε. αποτελεί η ενιαία πολιτική κυβερνοασφάλειας της οντότητας. Ο Υ.Α.Σ.Π.Ε. εποπτεύει την κατάρτιση, την εφαρμογή και την επικαιροποίησή της, διασφαλίζοντας ότι αυτή βασίζεται σε διεθνή πρότυπα και βέλτιστες πρακτικές και ότι ευθυγραμμίζεται με τις απαιτήσεις της ενωσιακής και εθνικής νομοθεσίας. Η πολιτική αυτή λειτουργεί ως το βασικό κανονιστικό πλαίσιο εσωτερικής διακυβέρνησης της κυβερνοασφάλειας, ενσωματώνοντας επιμέρους πολιτικές, διαδικασίες και μέτρα προστασίας.

Παράλληλα, ο Υ.Α.Σ.Π.Ε. διαδραματίζει κρίσιμο ρόλο στη διαχείριση κινδύνων και στην επιχειρησιακή συνέχεια. Είναι αρμόδιος για τον συντονισμό των διαδικασιών ανάλυσης κινδύνων, για τον σχεδιασμό και την εφαρμογή σχεδίων επιχειρησιακής συνέχειας και ανάκαμψης από καταστροφές, καθώς και για την τήρηση επικαιροποιημένου μητρώου πληροφοριακών και επικοινωνιακών αγαθών, τα οποία ιεραρχούνται βάσει της κρισιμότητάς τους. Η προσέγγιση αυτή αντανακλά την έμφαση της NIS 2 στην ανθεκτικότητα των οντοτήτων και στην ικανότητά τους να συνεχίζουν τη λειτουργία τους ακόμη και υπό συνθήκες σοβαρών κυβερνοπεριστατικών.

Ιδιαίτερη βαρύτητα αποδίδεται επίσης στη διαχείριση της ασφάλειας της αλυσίδας εφοδιασμού, καθώς ο Υ.Α.Σ.Π.Ε. μεριμνά για την ενσωμάτωση απαιτήσεων κυβερνοασφάλειας ήδη από το στάδιο των προμηθειών εξοπλισμού και υπηρεσιών ΤΠΕ και καθ' όλο τον κύκλο ζωής των σχετικών συμβάσεων. Η αρμοδιότητα αυτή συνδέεται άμεσα με τη NIS 2, η οποία εισάγει αυξημένες υποχρεώσεις για τον έλεγχο και τον περιορισμό των κινδύνων που απορρέουν από τρίτους παρόχους.

Ο νομοθέτης προβλέπει ρητώς ασυμβίβαστα καθήκοντα, προκειμένου να διασφαλιστεί η ανεξαρτησία και η αμεροληψία του Υ.Α.Σ.Π.Ε. Ειδικότερα, τα καθήκοντά του είναι ασυμβίβαστα με αυτά του Υπευθύνου Προστασίας Δεδομένων (Υ.Π.Δ.), καθώς και με ρόλους που σχετίζονται με τη διαχείριση των Τεχνολογιών Πληροφορικής και Επικοινωνιών ή της ηλεκτρονικής διακυβέρνησης. Η πρόβλεψη αυτή υπογραμμίζει τη διάκριση μεταξύ προστασίας δεδομένων προσωπικού χαρακτήρα και κυβερνοασφάλειας, διασφαλίζοντας τη σαφή κατανομή αρμοδιοτήτων και την αποφυγή σύγκρουσης συμφερόντων.

Σε επίπεδο προσόντων, ο Υ.Α.Σ.Π.Ε. οφείλει να διαθέτει επαρκή γνώση των επιχειρησιακών διαδικασιών της οντότητας και αποδεδειγμένη εξειδίκευση στους τομείς της ασφάλειας πληροφοριών και δικτύων ή της κυβερνοασφάλειας, είτε μέσω ακαδημαϊκών τίτλων είτε μέσω πολυετούς επαγγελματικής εμπειρίας ή πιστοποιημένης γνώσης διεθνών προτύπων και μεθοδολογιών. Παράλληλα, θεσπίζονται αυστηρά κωλύματα διορισμού και υποχρεώσεις ελέγχου ακεραιότητας, στοιχείο που ενισχύει την αξιοπιστία του θεσμού και την εμπιστοσύνη των αρμόδιων αρχών.

Συνολικά, ο Υ.Α.Σ.Π.Ε./CISO, όπως διαμορφώνεται στο πλαίσιο της NIS 2 και του ν. 5160/2024, αποτελεί τον θεμελιώδη σύνδεσμο μεταξύ τεχνικής ασφάλειας, οργανωτικής διακυβέρνησης και κανονιστικής συμμόρφωσης. Ο ρόλος του υπερβαίνει την παραδοσιακή τεχνική διάσταση της ασφάλειας πληροφοριακών συστημάτων και εντάσσεται πλέον στον πυρήνα της στρατηγικής διοίκησης των βασικών και σημαντικών οντοτήτων, συμβάλλοντας καθοριστικά στην ενίσχυση της εθνικής και ενωσιακής κυβερνοανθεκτικότητας, όπως αυτή επιδιώκεται από την Οδηγία NIS 2.

5.3 Ρόλος, αρμοδιότητες και τρόποι άσκησης ελέγχου του Υπεύθυνου Ασφάλειας Συστημάτων Πληροφορικής και Επικοινωνιών (Υ.Α.Σ.Π.Ε.) / CISO εντός του οργανισμού

Ο Υπεύθυνος Ασφάλειας Συστημάτων Πληροφορικής και Επικοινωνιών (Υ.Α.Σ.Π.Ε.), αντίστοιχος του Chief Information Security Officer (CISO) στη διεθνή πρακτική, αποτελεί κεντρικό θεσμό εσωτερικής διακυβέρνησης της κυβερνοασφάλειας στο πλαίσιο της Οδηγίας (ΕΕ) 2022/2555 (NIS 2). Η θεσμοθέτησή του στο εθνικό δίκαιο, ιδίως με τον ν. 5160/2024 και τις κανονιστικές πράξεις εφαρμογής του, αποτυπώνει τη σαφή βούληση του νομοθέτη να ενσωματώσει την κυβερνοασφάλεια στον πυρήνα της οργανωτικής και διοικητικής λειτουργίας των βασικών και σημαντικών οντοτήτων, αναγνωρίζοντάς την ως διαρκή και οριζόντια επιχειρησιακή προτεραιότητα.

Ο ρόλος του Υ.Α.Σ.Π.Ε. είναι κατ' εξοχήν στρατηγικός, συντονιστικός και ελεγκτικός. Δεν περιορίζεται στη διαχείριση τεχνικών ζητημάτων ασφάλειας πληροφοριακών συστημάτων, αλλά εκτείνεται στη διαμόρφωση, εποπτεία και αξιολόγηση του συνολικού πλαισίου κυβερνοασφάλειας του οργανισμού. Ο Υ.Α.Σ.Π.Ε.

λειτουργεί ως ο βασικός σύνδεσμος μεταξύ της τεχνικής λειτουργίας των συστημάτων ΤΠΕ, της διοίκησης του οργανισμού και των αρμόδιων εθνικών αρχών κυβερνοασφάλειας, διασφαλίζοντας τη συνεκτικότητα των ενεργειών και τη συμμόρφωση με τις κανονιστικές απαιτήσεις.

Οι αρμοδιότητες του Υ.Α.Σ.Π.Ε. καλύπτουν όλο το φάσμα της διαχείρισης κινδύνων κυβερνοασφάλειας. Καταρχάς, φέρει τη διαρκή ευθύνη εποπτείας της ασφάλειας των δικτύων και των πληροφοριακών συστημάτων του οργανισμού, καθώς και της υλοποίησης των τεχνικών και οργανωτικών μέτρων προστασίας. Στο πλαίσιο αυτό, παρακολουθεί την εφαρμογή πολιτικών ασφάλειας, διαδικασιών, ελέγχων πρόσβασης, μηχανισμών ανίχνευσης περιστατικών και μέτρων προστασίας από κακόβουλες ενέργειες, αξιολογώντας την αποτελεσματικότητά τους σε συνάρτηση με το επίπεδο απειλών και την κρισιμότητα των υποδομών.

Κεντρική αρμοδιότητα του Υ.Α.Σ.Π.Ε. αποτελεί η κατάρτιση, εφαρμογή και επικαιροποίηση της ενιαίας πολιτικής κυβερνοασφάλειας του οργανισμού. Η πολιτική αυτή λειτουργεί ως δεσμευτικό εσωτερικό κανονιστικό πλαίσιο, εντός του οποίου εντάσσονται όλες οι επιμέρους πολιτικές και διαδικασίες ασφάλειας. Ο Υ.Α.Σ.Π.Ε. διασφαλίζει ότι η πολιτική κυβερνοασφάλειας ευθυγραμμίζεται με διεθνή πρότυπα και βέλτιστες πρακτικές, ανταποκρίνεται στις απαιτήσεις της NIS 2 και εγκρίνεται από τα όργανα διοίκησης, τα οποία φέρουν την τελική ευθύνη για την εφαρμογή της.

Ιδιαίτερης σημασίας είναι ο ρόλος του Υ.Α.Σ.Π.Ε. στη διαχείριση περιστατικών κυβερνοασφάλειας**.** Ο Υ.Α.Σ.Π.Ε. συντονίζει τις εσωτερικές διαδικασίες απόκρισης σε περιστατικά, εξασφαλίζοντας την έγκαιρη ανίχνευση, ανάλυση, περιορισμό και αποκατάσταση των επιπτώσεων. Παράλληλα, επιμελείται τη συμμόρφωση του οργανισμού με τις υποχρεώσεις κοινοποίησης σημαντικών περιστατικών προς τις αρμόδιες αρχές και τα CSIRT, όπως προβλέπει η NIS 2, λειτουργώντας ως σημείο επαφής και διασφαλίζοντας την ακρίβεια, πληρότητα και έγκαιρη υποβολή των σχετικών πληροφοριών.

Ο Υ.Α.Σ.Π.Ε. διαδραματίζει επίσης καίριο ρόλο στη διαχείριση κινδύνων και στην επιχειρησιακή ανθεκτικότητα. Είναι υπεύθυνος για τον συντονισμό των διαδικασιών ανάλυσης και αξιολόγησης κινδύνων κυβερνοασφάλειας, λαμβάνοντας υπόψη τόσο εσωτερικές όσο και εξωτερικές απειλές, καθώς και κινδύνους που απορρέουν από την

αλυσίδα εφοδιασμού. Στο πλαίσιο αυτό, μεριμνά για την ανάπτυξη και εφαρμογή σχεδίων επιχειρησιακής συνέχειας και ανάκαμψης από καταστροφές, εξασφαλίζοντας ότι ο οργανισμός είναι σε θέση να διατηρήσει ή να αποκαταστήσει κρίσιμες λειτουργίες ακόμη και σε περίπτωση σοβαρών κυβερνοπεριστατικών.

Οι τρόποι άσκησης ελέγχου του Υ.Α.Σ.Π.Ε. εντός του οργανισμού είναι κυρίως οργανωτικοί, διαδικαστικοί και εποπτικοί. Ο Υ.Α.Σ.Π.Ε. δεν ασκεί έλεγχο με πειθαρχικό ή ιεραρχικό χαρακτήρα, αλλά μέσω της θέσπισης πολιτικών, της παρακολούθησης της συμμόρφωσης και της συστηματικής αξιολόγησης της αποτελεσματικότητας των μέτρων ασφάλειας. Μέσω τακτικών εσωτερικών ελέγχων, αναφορών, δεικτών απόδοσης ασφάλειας (security metrics) και αναλύσεων κινδύνου, αξιολογεί το επίπεδο κυβερνοασφάλειας των επιμέρους οργανικών μονάδων και εισηγείται διορθωτικές ενέργειες προς τη διοίκηση.

Παράλληλα, ο Υ.Α.Σ.Π.Ε. ασκεί έλεγχο μέσω της ενημέρωσης και ευαισθητοποίησης του ανθρώπινου δυναμικού και των οργάνων διοίκησης. Η εκπαίδευση στελεχών και εργαζομένων σε θέματα κυβερνοασφάλειας αποτελεί βασικό εργαλείο πρόληψης και συμμόρφωσης, ιδίως σε σχέση με απειλές κοινωνικής μηχανικής και ανθρώπινου σφάλματος. Η τακτική παρουσίαση της στρατηγικής κυβερνοασφάλειας και των υφιστάμενων κινδύνων στη διοίκηση επιτρέπει τη λήψη τεκμηριωμένων αποφάσεων και ενισχύει τη λογοδοσία, όπως επιτάσσει η NIS 2.

Επιπλέον, ο Υ.Α.Σ.Π.Ε. συμμετέχει ενεργά σε ελέγχους και επιθεωρήσεις που διενεργούνται από αρμόδιες εθνικές αρχές ή πιστοποιημένους επιθεωρητές, παρέχοντας στοιχεία, τεκμηρίωση και πρόσβαση στα συστήματα, όπου απαιτείται. Μέσω της συνεργασίας αυτής, διασφαλίζεται η διαφάνεια, η αξιοπιστία και η συνεχής βελτίωση του επιπέδου κυβερνοασφάλειας του οργανισμού.

Συνολικά, ο Υ.Α.Σ.Π.Ε./CISO ενσαρκώνει το πρότυπο του σύγχρονου εσωτερικού ελεγκτικού και συντονιστικού μηχανισμού κυβερνοασφάλειας που προωθεί η NIS 2. Ο ρόλος του γεφυρώνει την τεχνική διάσταση της ασφάλειας πληροφοριακών συστημάτων με τη διοικητική διακυβέρνηση και τη νομική συμμόρφωση, καθιστώντας την κυβερνοασφάλεια αναπόσπαστο στοιχείο της οργανωτικής λειτουργίας και της στρατηγικής βιωσιμότητας των οργανισμών.

5.4 Προσόντα και στις πιστοποιήσεις που δύναται ή ενδείκνυται να διαθέτει ο Υπεύθυνος Ασφάλειας Συστημάτων Πληροφορικής και Επικοινωνιών (Υ.Α.Σ.Π.Ε.) / CISO

Η αποτελεσματική άσκηση των καθηκόντων του Υπεύθυνου Ασφάλειας Συστημάτων Πληροφορικής και Επικοινωνιών (Υ.Α.Σ.Π.Ε.), ο οποίος αντιστοιχεί λειτουργικά στον ρόλο του Chief Information Security Officer (CISO), προϋποθέτει υψηλό επίπεδο επιστημονικής κατάρτισης, επαγγελματικής εμπειρίας και εξειδικευμένων δεξιοτήτων. Η Οδηγία (ΕΕ) 2022/2555 (NIS 2), σε συνδυασμό με τον ν. 5160/2024 και τις κανονιστικές πράξεις εφαρμογής του, δεν περιορίζεται σε τυπικές απαιτήσεις ορισμού ενός υπευθύνου, αλλά επιβάλλει ουσιαστικά κριτήρια επάρκειας, ώστε ο Υ.Α.Σ.Π.Ε. να είναι σε θέση να ανταποκριθεί στον στρατηγικό, συντονιστικό και ελεγκτικό χαρακτήρα του ρόλου του.

Καταρχάς, βασικό προσόν του Υ.Α.Σ.Π.Ε. αποτελεί η επιστημονική κατάρτιση σε γνωστικά αντικείμενα συναφή με την ασφάλεια πληροφοριών, την κυβερνοασφάλεια ή τις τεχνολογίες πληροφορικής και επικοινωνιών. Η κατοχή προπτυχιακού ή μεταπτυχιακού τίτλου σπουδών σε τομείς όπως η Πληροφορική, η Μηχανική Υπολογιστών, η Ασφάλεια Πληροφοριακών Συστημάτων, η Κυβερνοασφάλεια ή συναφή πεδία θεωρείται ιδιαιτέρως σημαντική, καθώς παρέχει το αναγκαίο θεωρητικό υπόβαθρο για την κατανόηση της αρχιτεκτονικής των συστημάτων, των απειλών και των μηχανισμών προστασίας. Παράλληλα, η επαρκής γνώση των επιχειρησιακών διαδικασιών του οργανισμού αποτελεί κρίσιμο στοιχείο, δεδομένου ότι η κυβερνοασφάλεια δεν λειτουργεί αποκομμένα από τις επιχειρησιακές και διοικητικές λειτουργίες.

Πέραν της τυπικής εκπαίδευσης, η επαγγελματική εμπειρία στους τομείς της ασφάλειας πληροφοριών και δικτύων ή της κυβερνοασφάλειας αποτελεί καθοριστικό παράγοντα καταλληλότητας. Η πολυετής ενασχόληση με αντικείμενα όπως η διαχείριση κινδύνων, η ανάλυση και αντιμετώπιση περιστατικών, η εφαρμογή πολιτικών ασφάλειας και η συμμόρφωση με κανονιστικά πλαίσια επιτρέπει στον Υ.Α.Σ.Π.Ε. να αντιμετωπίζει σύνθετες καταστάσεις, να λαμβάνει τεκμηριωμένες αποφάσεις και να συντονίζει αποτελεσματικά ετερογενείς ομάδες και οργανικές μονάδες. Στο πλαίσιο της NIS 2, η

εμπειρία αυτή αποκτά ιδιαίτερη σημασία, καθώς οι οντότητες καλούνται να εφαρμόσουν ολιστικές προσεγγίσεις διαχείρισης κινδύνων και ανθεκτικότητας.

Ιδιαίτερο ρόλο διαδραματίζουν οι επαγγελματικές πιστοποιήσεις, οι οποίες λειτουργούν ως αντικειμενικός δείκτης εξειδικευμένης γνώσης και διεθνούς αναγνώρισης επαγγελματικής επάρκειας. Ενδεικτικά, πιστοποιήσεις στρατηγικού και διοικητικού χαρακτήρα, όπως οι πιστοποιήσεις CISSP (Certified Information Systems Security Professional) και CISM (Certified Information Security Manager), θεωρούνται ιδιαιτέρως συναφείς με τον ρόλο του Υ.Α.Σ.Π.Ε., καθώς εστιάζουν στη διακυβέρνηση της ασφάλειας πληροφοριών, στη διαχείριση κινδύνων και στην ευθυγράμμιση της ασφάλειας με τους επιχειρησιακούς στόχους. Αντίστοιχα, πιστοποιήσεις όπως η ISO/IEC 27001 Lead Implementer ή Lead Auditor παρέχουν τεκμηριωμένη γνώση για την ανάπτυξη, εφαρμογή και έλεγχο συστημάτων διαχείρισης ασφάλειας πληροφοριών, στοιχείο άμεσα συνδεδεμένο με τις απαιτήσεις της NIS 2.

Σε πιο τεχνικό επίπεδο, πιστοποιήσεις όπως οι CEH (Certified Ethical Hacker), GCIS/GCED/GCIA (SANS/GIAC) ή αντίστοιχες, ενισχύουν την ικανότητα του Υ.Α.Σ.Π.Ε. να κατανοεί σε βάθος τις τεχνικές επίθεσης και άμυνας, διευκολύνοντας την αποτελεσματική εποπτεία τεχνικών ομάδων και την αξιολόγηση της επάρκειας των εφαρμοζόμενων μέτρων ασφαλείας. Παρότι ο ρόλος του Υ.Α.Σ.Π.Ε. δεν είναι κατ' ανάγκη επιχειρησιακά τεχνικός, η τεχνική κατανόηση αποτελεί κρίσιμη προϋπόθεση για την ορθή λήψη αποφάσεων και την αξιόπιστη επικοινωνία με εξειδικευμένο προσωπικό.

Επιπλέον, ιδιαίτερη αξία έχουν πιστοποιήσεις και γνώσεις που αφορούν τη συμμόρφωση και το κανονιστικό πλαίσιο, όπως η κατανόηση της NIS 2, του Γενικού Κανονισμού για την Προστασία Δεδομένων (ΓΚΠΔ), καθώς και συναφών εθνικών και ενωσιακών νομοθετημάτων. Η διασύνδεση κυβερνοασφάλειας και κανονιστικής συμμόρφωσης καθιστά αναγκαία την κατοχή νομικο-διοικητικής αντίληψης, ώστε ο Υ.Α.Σ.Π.Ε. να μπορεί να μεταφράζει νομικές απαιτήσεις σε πρακτικά μέτρα ασφάλειας και εσωτερικές διαδικασίες.

Πέραν των τυπικών προσόντων και πιστοποιήσεων, ο ρόλος του Υ.Α.Σ.Π.Ε. προϋποθέτει ανεπτυγμένες οριζόντιες δεξιότητες, όπως ικανότητα στρατηγικού σχεδιασμού, διαχείρισης κρίσεων, λήψης αποφάσεων υπό πίεση, επικοινωνίας με τη διοίκηση και συντονισμού πολλαπλών εμπλεκόμενων μερών. Οι δεξιότητες αυτές είναι

ιδιαιτέρως κρίσιμες στο πλαίσιο της NIS 2, η οποία ενισχύει τη λογοδοσία των οργάνων διοίκησης και απαιτεί τη συστηματική ενημέρωσή τους από τον Υ.Α.Σ.Π.Ε. για τους κινδύνους και τις κυβερνοαπειλές.

Συνολικά, τα προσόντα και οι πιστοποιήσεις του Υ.Α.Σ.Π.Ε./CISO δεν αποτελούν απλώς τυπικές προϋποθέσεις διορισμού, αλλά ουσιώδη στοιχεία διασφάλισης της αποτελεσματικής εφαρμογής της NIS 2 σε επίπεδο οργανισμού. Ο συνδυασμός επιστημονικής γνώσης, επαγγελματικής εμπειρίας, διεθνώς αναγνωρισμένων πιστοποιήσεων και διοικητικών δεξιοτήτων καθιστά τον Υ.Α.Σ.Π.Ε. βασικό πυλώνα της σύγχρονης διακυβέρνησης κυβερνοασφάλειας και εγγυητή της ανθεκτικότητας των κρίσιμων και σημαντικών οντοτήτων.

6. ΔΙΑΧΕΙΡΙΣΗ ΕΠΙΚΙΝΔΥΝΟΤΗΤΑΣ ΣΤΟΝ ΤΟΜΕΑ ΤΗΣ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ – ΤΕΧΝΙΚΑ ΚΑΙ ΟΡΓΑΝΩΤΙΚΑ ΜΕΤΡΑ ΑΣΦΑΛΕΙΑΣ ΣΤΟ ΠΛΑΙΣΙΟ ΣΥΜΜΟΡΦΩΣΗΣ ΜΕ ΤΗΝ ΟΔΗΓΙΑ NIS2 ΚΑΙ ΤΟΝ Ν. 5160/2024

6.1 Πλαίσιο διαχείρισης κινδύνων κυβερνοασφάλειας

Η διαχείριση επικινδυνότητας στον τομέα της κυβερνοασφάλειας αποτελεί τον θεμέλιο λίθο της σύγχρονης προσέγγισης ασφάλειας δικτύων και πληροφοριακών συστημάτων και προϋπόθεση για τη λήψη κατάλληλων, αναλογικών και αποτελεσματικών μέτρων προστασίας από τις υπόχρεες οντότητες. Στο πλαίσιο της Οδηγίας (ΕΕ) 2022/2555 (NIS 2) και της ενσωμάτωσής της στο εθνικό δίκαιο με τον ν. 5160/2024, η κυβερνοασφάλεια δεν αντιμετωπίζεται ως σύνολο αποσπασματικών τεχνικών λύσεων, αλλά ως δομημένη διαδικασία διακυβέρνησης κινδύνων, η οποία προηγείται και καθοδηγεί κάθε απόφαση λήψης μέτρων.

Η διαδικασία αυτή εντάσσεται σε ένα ευρύτερο πλαίσιο διοίκησης κυβερνοασφάλειας, στο οποίο ο οργανισμός οφείλει να έχει θεσπίσει σαφείς ρόλους και ευθύνες, διακριτή οργανική μονάδα αρμόδια για την ασφάλεια πληροφοριακών συστημάτων και ενεργή εμπλοκή της ανώτατης διοίκησης. Η διαχείριση επικινδυνότητας

δεν αποτελεί αποκλειστικά τεχνική άσκηση, αλλά διοικητική και στρατηγική λειτουργία, η οποία υποστηρίζεται από καταγεγραμμένες και εγκεκριμένες πολιτικές ασφάλειας, επαρκείς πόρους και μηχανισμούς λογοδοσίας.

Πριν από τη λήψη οποιουδήποτε τεχνικού, οργανωτικού ή επιχειρησιακού μέτρου κυβερνοασφάλειας, οι υπόχρεες οντότητες οφείλουν να διενεργούν διαδικασίες αποτίμησης επικινδυνότητας (risk assessment). Στο πλαίσιο αυτό, εντοπίζονται, αναλύονται και αξιολογούνται οι κίνδυνοι που απειλούν τα συστήματα δικτύου και πληροφοριών, λαμβάνοντας υπόψη τόσο το τεχνικό περιβάλλον όσο και το οργανωσιακό, επιχειρησιακό και νομικό πλαίσιο εντός του οποίου λειτουργεί ο οργανισμός. Η αποτίμηση επικινδυνότητας ενεργοποιείται ιδίως όταν λαμβάνουν χώρα σημαντικές τεχνικές αλλαγές στα πληροφοριακά συστήματα που υποστηρίζουν κρίσιμες υπηρεσίες ή όταν μεταβάλλεται ουσιωδώς το περιβάλλον κυβερνοαπειλών.

Η προσέγγιση που υιοθετείται είναι κατ' ανάγκη risk-based, δηλαδή βασισμένη στον κίνδυνο. Οι οντότητες καλούνται να αξιολογούν συστηματικά την πιθανότητα εκδήλωσης απειλών και τη σοβαρότητα των συνεπειών τους, όχι μόνο ως προς τη λειτουργική συνέχεια του οργανισμού, αλλά και ως προς τις κοινωνικές, οικονομικές και, κατά περίπτωση, διασυστημικές επιπτώσεις. Η αναλογικότητα των μέτρων που θα ληφθούν κρίνεται με βάση τον βαθμό έκθεσης της οντότητας σε κινδύνους, το μέγεθός της, την κρισιμότητα των παρεχόμενων υπηρεσιών και τη δυνητική επίδραση ενός περιστατικού στους αποδέκτες των υπηρεσιών ή σε άλλους οργανισμούς.

Κεντρικό στοιχείο της διαδικασίας αποτελεί η τεκμηρίωση της επικινδυνότητας. Οι οργανισμοί οφείλουν να διατηρούν καταγεγραμμένα αποτελέσματα της αποτίμησης κινδύνων, τα οποία αποτυπώνονται συχνά σε πίνακες εκτίμησης επικινδυνότητας (risk matrices ή risk registers). Στους πίνακες αυτούς καταγράφονται τα πληροφοριακά αγαθά, οι απειλές, οι ευπάθειες, οι πιθανότητες υλοποίησης και οι επιπτώσεις, καθώς και το υπολειπόμενο επίπεδο κινδύνου μετά την εφαρμογή υφιστάμενων μέτρων. Η τεκμηρίωση αυτή δεν έχει μόνο εσωτερική αξία, αλλά λειτουργεί και ως αποδεικτικό στοιχείο συμμόρφωσης έναντι των αρμόδιων εποπτικών αρχών.

Η διαχείριση επικινδυνότητας δεν περιορίζεται στον εντοπισμό και την αξιολόγηση κινδύνων, αλλά περιλαμβάνει και τη λήψη αποφάσεων για τη μεταχείρισή τους. Στο στάδιο αυτό, ο οργανισμός καλείται να επιλέξει, με τεκμηριωμένο τρόπο, εάν

θα μετριάσει τον κίνδυνο μέσω τεχνικών και οργανωτικών μέτρων, εάν θα τον αποδεχθεί, εάν θα τον μεταφέρει (π.χ. μέσω συμβάσεων ή ασφαλιστικών μηχανισμών) ή εάν θα αποφύγει τη δραστηριότητα που τον προκαλεί. Οι αποφάσεις αυτές λαμβάνονται σε επίπεδο διοίκησης και βασίζονται στα αποτελέσματα της αποτίμησης επικινδυνότητας, στο κόστος εφαρμογής των μέτρων και στη στρατηγική σημασία των προστατευόμενων συστημάτων.

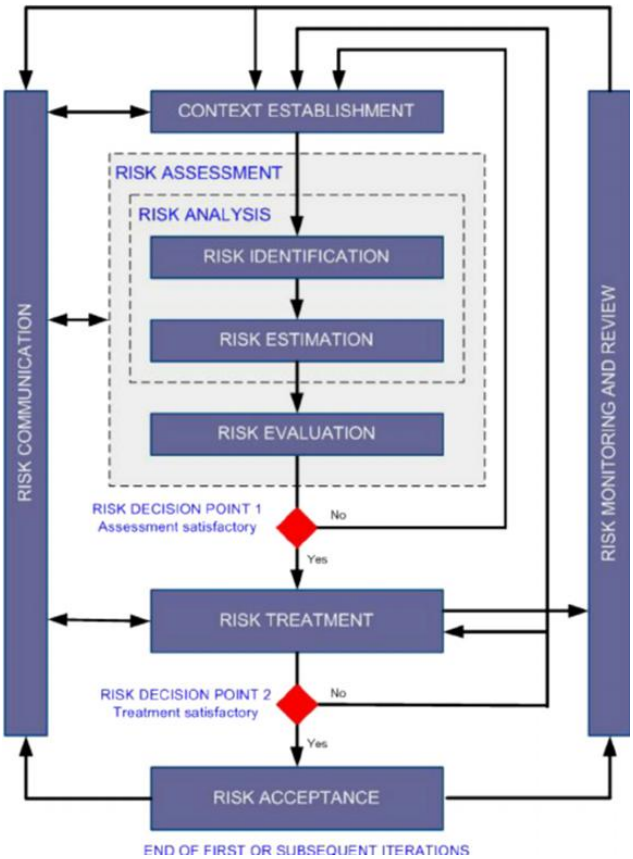
Ιδιαίτερη έμφαση δίνεται στην ολιστική προσέγγιση του κινδύνου, όπως απαιτείται από το άρθρο 15 του ν. 5160/2024 και την NIS 2. Τα μέτρα που τελικώς θα ληφθούν πρέπει να καλύπτουν όχι μόνο την τεχνική ασφάλεια των συστημάτων, αλλά και το φυσικό περιβάλλον, τον ανθρώπινο παράγοντα, την αλυσίδα εφοδιασμού και τις διαδικασίες επιχειρησιακής συνέχειας. Στο πλαίσιο αυτό, η αποτίμηση επικινδυνότητας προηγείται της επιλογής μέτρων όπως η διαχείριση περιστατικών, η ασφάλεια προμηθευτών, η κρυπτογραφία, η πολυπαραγοντική αυθεντικοποίηση, η κυβερνοϋγιεινή και η εκπαίδευση προσωπικού.

Η εφαρμογή της διαχείρισης επικινδυνότητας υποστηρίζεται από διεθνώς αναγνωρισμένα πρότυπα και μεθοδολογίες. Ενδεικτικά, το ISO 31000 παρέχει το γενικό πλαίσιο αρχών και κατευθυντήριων γραμμών για τη διαχείριση κινδύνων σε οργανωσιακό επίπεδο, ενώ το ISO/IEC 27005 εξειδικεύει τη διαχείριση κινδύνων ασφάλειας πληροφοριών στο πλαίσιο ενός Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών (ISMS). Παράλληλα, πρότυπα και πλαίσια όπως το ISO/IEC 27001, το NIST Cybersecurity Framework, το ISA/IEC 62443 και το PCI DSS συμβάλλουν στη διαμόρφωση δομημένων και επαναλήψιμων διαδικασιών αποτίμησης και αντιμετώπισης κινδύνων, ανάλογα με τον τομέα δραστηριότητας και το επίπεδο ωριμότητας του οργανισμού.

Η διαχείριση επικινδυνότητας αποτελεί δυναμική και επαναλαμβανόμενη διαδικασία. Οι οργανισμοί οφείλουν να αξιολογούν περιοδικά την αποτελεσματικότητα των διαδικασιών risk assessment, να αναθεωρούν τις παραδοχές τους και να ενσωματώνουν νέα δεδομένα, ιδίως πληροφορίες κυβερνοαπειλών που προκύπτουν από προγράμματα cyber threat intelligence. Τα αποτελέσματα και τα συμπεράσματα της αποτίμησης επικινδυνότητας κοινοποιούνται εγκαίρως σε πρόσωπα με αρμοδιότητα λήψης αποφάσεων και λογοδοσίας, ενώ η απόδοση των πολιτικών και των διαδικασιών

κυβερνοασφάλειας αξιολογείται μέσω βασικών δεικτών απόδοσης, τα αποτελέσματα των οποίων γνωστοποιούνται στην ανώτατη διοίκηση.

Συνολικά, η διαχείριση επικινδυνότητας συνιστά το αναγκαίο προπαρασκευαστικό στάδιο πριν από τη λήψη μέτρων κυβερνοασφάλειας και τον βασικό μηχανισμό μέσω του οποίου οι υπόχρεες οντότητες διασφαλίζουν ότι τα μέτρα που εφαρμόζουν είναι τεκμηριωμένα, αναλογικά και ευθυγραμμισμένα με το πραγματικό επίπεδο κινδύνου. Η προσέγγιση αυτή αντανακλά πλήρως τη φιλοσοφία της NIS 2, η οποία μετατοπίζει το επίκεντρο της κυβερνοασφάλειας από την αποσπασματική συμμόρφωση στη συστηματική διακυβέρνηση κινδύνων και στην ενίσχυση της οργανωσιακής ανθεκτικότητας.



Διαδικασία διαχείρισης επικινδυνότητας ασφάλειας πληροφοριών σύμφωνα με τα πρότυπα ISO 31000 και ISO/IEC 27005

Το ανωτέρω σχήμα απεικονίζει τη δομημένη και επαναληπτική διαδικασία διαχείρισης επικινδυνότητας, όπως αυτή περιγράφεται στα διεθνή πρότυπα ISO 31000 και

ISO/IEC 27005. Η διαδικασία ξεκινά με τον καθορισμό του πλαισίου λειτουργίας του οργανισμού και ακολουθείται από τη συστηματική αναγνώριση, ανάλυση και αξιολόγηση των κινδύνων. Βάσει των αποτελεσμάτων αυτών, λαμβάνονται αποφάσεις για την αντιμετώπιση των κινδύνων μέσω κατάλληλων και αναλογικών μέτρων ασφάλειας. Η διαδικασία υποστηρίζεται διαρκώς από μηχανισμούς επικοινωνίας και διαβούλευσης, καθώς και από συνεχή παρακολούθηση και αναθεώρηση, διασφαλίζοντας την προσαρμογή της στις μεταβαλλόμενες απειλές και απαιτήσεις. Στο πλαίσιο της Οδηγίας (ΕΕ) 2022/2555 (NIS 2), η ανωτέρω προσέγγιση αποτελεί αναγκαία προϋπόθεση για την τεκμηρίωση της αναλογικότητας και της επάρκειας των μέτρων κυβερνοασφάλειας που υιοθετούν οι υπόχρεες οντότητες.

6.2 Τεχνικά και Οργανωτικά Μέτρα Ασφάλειας στο πλαίσιο συμμόρφωσης με την Οδηγία NIS2 και τον ν. 5160/2024

Σε εφαρμογή του θεσμικού πλαισίου που θεσπίστηκε σε ενωσιακό και εθνικό επίπεδο για την ενίσχυση της κυβερνοασφάλειας, η Οδηγία (ΕΕ) 2022/2555 (NIS2) και ο ν. 5160/2024 εισάγουν ένα συνεκτικό και δεσμευτικό σύστημα υποχρεώσεων για τις βασικές και σημαντικές οντότητες, με έμφαση στη συστηματική διαχείριση κινδύνων και στην υιοθέτηση κατάλληλων τεχνικών και οργανωτικών μέτρων ασφάλειας. Το νέο αυτό πλαίσιο σηματοδοτεί τη μετάβαση από μια αποσπασματική προσέγγιση προστασίας πληροφοριακών συστημάτων σε ένα ολοκληρωμένο μοντέλο πρόληψης, ανθεκτικότητας και επιχειρησιακής ετοιμότητας έναντι κυβερνοαπειλών.

Ειδικότερα, το άρθρο 21 της Οδηγίας NIS2 καθιερώνει την υποχρέωση των υπόχρεων οντοτήτων να λαμβάνουν μέτρα διαχείρισης κινδύνων κυβερνοασφάλειας, τα οποία είναι κατάλληλα και αναλογικά προς το προφίλ κινδύνου κάθε οντότητας, λαμβάνοντας υπόψη τη φύση των δραστηριοτήτων της, το μέγεθός της, τον βαθμό έκθεσης σε απειλές και τις πιθανές κοινωνικές και οικονομικές επιπτώσεις ενός περιστατικού. Οι υποχρεώσεις αυτές εξειδικεύονται περαιτέρω στο εθνικό δίκαιο μέσω του ν. 5160/2024, ο οποίος θεσπίζει το πλαίσιο εφαρμογής, εποπτείας και επιβολής των εν λόγω μέτρων στην Ελλάδα.

Υπό αυτά τα δεδομένα, καθοριστικό ρόλο διαδραματίζει η Υπουργική Απόφαση υπ' αριθμ. 1689/2025, με την οποία θεσπίζεται το «Εθνικό Πλαίσιο Απαιτήσεων Κυβερνοασφάλειας Βασικών και Σημαντικών Οντοτήτων». Η εν λόγω απόφαση λειτουργεί ως κανονιστικό εργαλείο εξειδίκευσης των γενικών υποχρεώσεων της NIS2 και του ν. 5160/2024, προσδιορίζοντας με μεγαλύτερη σαφήνεια τις επιμέρους πολιτικές, διαδικασίες και μέτρα ασφάλειας που υποχρεούνται να υιοθετούν και να εφαρμόζουν οι υπόχρεες οντότητες. Μέσω του Εθνικού Πλαισίου, οι αφηρημένες κανονιστικές απαιτήσεις μεταφράζονται σε συγκεκριμένες, εφαρμόσιμες και ελέγξιμες πρακτικές.

Τα τεχνικά και οργανωτικά μέτρα ασφάλειας που προβλέπονται στο εν λόγω πλαίσιο καλύπτουν ένα ευρύ φάσμα τομέων, όπως η ανάλυση και διαχείριση κινδύνων, η ασφάλεια πληροφοριακών συστημάτων και δικτύων, η διαχείριση περιστατικών κυβερνοασφάλειας, η επιχειρησιακή συνέχεια και η ανάκαμψη από καταστροφή, η ασφάλεια της εφοδιαστικής αλυσίδας, η κρυπτογραφία, ο έλεγχος πρόσβασης, η ασφάλεια ανθρώπινων πόρων και η εκπαίδευση προσωπικού. Τα μέτρα αυτά δεν αντιμετωπίζονται ως απομονωμένες τεχνικές λύσεις, αλλά ως αλληλένδετα στοιχεία ενός συνολικού συστήματος διακυβέρνησης της κυβερνοασφάλειας.

Η παρούσα ενότητα αποσκοπεί στην εισαγωγική αποτύπωση του πλαισίου των τεχνικών και οργανωτικών μέτρων ασφάλειας που απορρέουν από την Οδηγία NIS2, τον ν. 5160/2024 και την Υπουργική Απόφαση 1689/2025. Η αναλυτική εξειδίκευση των επιμέρους πολιτικών, διαδικασιών και μέτρων, καθώς και η παρουσίαση των απαιτήσεων συμμόρφωσης για τις βασικές και σημαντικές οντότητες, πραγματοποιείται σε επόμενες υποενότητες του παρόντος κεφαλαίου που ακολουθούν.

6.2.1 Πολιτικές και διαδικασίες ασφάλειας πληροφοριών

Οι πολιτικές και οι διαδικασίες ασφάλειας πληροφοριών αποτελούν βασικό πυλώνα της οργανωτικής και λειτουργικής προσέγγισης των βασικών και σημαντικών οντοτήτων στον τομέα της κυβερνοασφάλειας. Η υιοθέτησή τους δεν περιορίζεται σε τεχνικές ρυθμίσεις, αλλά συνιστά στοιχείο συνολικής διακυβέρνησης της ασφάλειας, καθώς καθορίζει τον τρόπο με τον οποίο η οντότητα διαχειρίζεται τους κινδύνους που σχετίζονται με τα συστήματα δικτύου και πληροφοριών της.

Στο πλαίσιο αυτό, κάθε οντότητα οφείλει να εκπονεί γραπτή γενική πολιτική ασφάλειας πληροφοριών, η οποία εγκρίνεται από το ανώτατο όργανο διοίκησης και αποτυπώνει τη στρατηγική προσέγγιση της οντότητας ως προς τη διαχείριση της ασφάλειας. Η γενική πολιτική λειτουργεί ως θεμέλιο για το σύνολο των επιμέρους ρυθμίσεων, καθορίζοντας τους στόχους, τις βασικές αρχές, τους ρόλους και τις αρμοδιότητες, καθώς και το επίπεδο αποδεκτού κινδύνου σε σχέση με την προστασία της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των πληροφοριών.

Πέραν της γενικής πολιτικής, οι βασικές και σημαντικές οντότητες υποχρεούνται να αναπτύσσουν γραπτές θεματικές πολιτικές ασφάλειας, οι οποίες καλύπτουν ειδικές πτυχές της κυβερνοασφάλειας και αφορούν το ανθρώπινο δυναμικό, τις οργανωτικές διαδικασίες και τις τεχνολογικές υποδομές. Οι θεματικές πολιτικές εγκρίνονται επίσης από το ανώτατο όργανο διοίκησης, γεγονός που ενισχύει τη θεσμική τους βαρύτητα και διασφαλίζει την ενσωμάτωσή τους στη συνολική στρατηγική της οντότητας.

Ενδεικτικά, το ελάχιστο σύνολο θεματικών πολιτικών που απαιτούνται περιλαμβάνει πολιτικές ελέγχου πρόσβασης, διαχείρισης αγαθών, ορθής χρήσης αγαθών και δεδομένων, διαχείρισης αφαιρούμενων μέσων αποθήκευσης, διαχείρισης περιστατικών κυβερνοασφάλειας, ασφάλειας της εφοδιαστικής αλυσίδας, ασφάλειας δικτύων, διενέργειας ελέγχων κυβερνοασφάλειας, αντιγράφων ασφαλείας, κρυπτογράφησης δεδομένων και επικοινωνιών, καθώς και φυσικής και περιβαλλοντικής ασφάλειας. Το πλαίσιο αυτό διασφαλίζει ότι καλύπτεται ένα ευρύ φάσμα κινδύνων, από τον ανθρώπινο παράγοντα έως τις τεχνικές και φυσικές απειλές.

Παράλληλα, παρέχεται στις οντότητες η δυνατότητα εκπόνησης πρόσθετων θεματικών πολιτικών, ανάλογα με τις ειδικές ανάγκες, το μέγεθος, τη φύση των δραστηριοτήτων τους και το επίπεδο έκθεσής τους σε κυβερνοκινδύνους. Η ευελιξία αυτή επιτρέπει την προσαρμογή του πλαισίου ασφάλειας στις ιδιαιτερότητες κάθε οργανισμού, χωρίς να υπονομεύεται η συμμόρφωση με τις ελάχιστες κανονιστικές απαιτήσεις.

Τέλος, τόσο η γενική πολιτική ασφάλειας πληροφοριών όσο και οι θεματικές πολιτικές υπόκεινται σε τακτική αξιολόγηση και, κατά περίπτωση, επικαιροποίηση. Η διαδικασία αυτή πραγματοποιείται σε προγραμματισμένα χρονικά διαστήματα, αλλά και εκτάκτως, όταν λαμβάνουν χώρα σοβαρά περιστατικά κυβερνοασφάλειας ή

σημαντικές αλλαγές στις λειτουργίες, στις υποδομές ή στο κανονιστικό περιβάλλον της οντότητας. Με τον τρόπο αυτό, διασφαλίζεται ότι το πλαίσιο πολιτικών παραμένει επίκαιρο, αποτελεσματικό και ευθυγραμμισμένο με τις εξελισσόμενες απειλές και απαιτήσεις, ενισχύοντας τη συνολική ανθεκτικότητα της οντότητας στον κυβερνοχώρο.

6.2.2 Ανεξάρτητος έλεγχος ασφάλειας πληροφοριών

Οι ανεξάρτητοι έλεγχοι ασφάλειας πληροφοριών αποτελούν βασικό μηχανισμό διασφάλισης της αποτελεσματικής εφαρμογής του προγράμματος διαχείρισης ασφάλειας πληροφοριών των βασικών οντοτήτων. Στο πλαίσιο αυτό, οι οντότητες υποχρεούνται να υλοποιούν, σε περιοδική βάση, ανεξάρτητους ελέγχους που καλύπτουν το σύνολο των παραμέτρων της κυβερνοασφάλειας, συμπεριλαμβανομένου του ανθρώπινου δυναμικού, των εφαρμοζόμενων πολιτικών, των οργανωτικών και επιχειρησιακών διαδικασιών, καθώς και των τεχνολογικών μέσων και υποδομών που χρησιμοποιούνται. Οι έλεγχοι αυτοί δύνανται να διενεργούνται είτε από εσωτερικούς είτε από εξωτερικούς ελεγκτές, υπό την προϋπόθεση ότι διασφαλίζεται ο ανεξάρτητος χαρακτήρας τους.

Ιδιαίτερη σημασία αποδίδεται στη διασφάλιση της αμεροληψίας και της αντικειμενικότητας των προσώπων που διενεργούν τους ανεξάρτητους ελέγχους. Η οντότητα οφείλει να λαμβάνει τα κατάλληλα οργανωτικά και διοικητικά μέτρα, ώστε οι ελεγκτές να μην επηρεάζονται από συγκρούσεις συμφερόντων ή ιεραρχικές εξαρτήσεις που θα μπορούσαν να υπονομεύσουν την αξιοπιστία των αποτελεσμάτων του ελέγχου.

Σε περιπτώσεις όπου από τα ευρήματα των ανεξάρτητων ελέγχων προκύπτει ανεπαρκής υλοποίηση ή αποτελεσματικότητα των αναγκαίων τεχνικών, οργανωτικών ή επιχειρησιακών μέτρων κυβερνοασφάλειας, ενεργοποιείται η ευθύνη του ανώτατου οργάνου διοίκησης της οντότητας. Το τελευταίο υποχρεούται να εκκινήσει διαδικασίες λήψης διορθωτικών και, κατά περίπτωση, προληπτικών ενεργειών, με στόχο την άρση των διαπιστωθεισών αδυναμιών και την ενίσχυση της συνολικής στάθμης ασφάλειας.

Οι ανεξάρτητοι έλεγχοι δεν περιορίζονται σε προκαθορισμένα χρονικά διαστήματα, αλλά δύνανται να διενεργούνται και εκτάκτως, όταν λαμβάνουν χώρα σοβαρά περιστατικά κυβερνοασφάλειας, όταν επέρχονται σημαντικές αλλαγές στις

λειτουργίες, στις υποδομές ή στο επιχειρησιακό μοντέλο της οντότητας, καθώς και όταν μεταβάλλεται ουσιωδώς το διεθνές περιβάλλον κυβερνοαπειλών. Η δυναμική αυτή προσέγγιση διασφαλίζει ότι το πρόγραμμα διαχείρισης ασφάλειας πληροφοριών παραμένει επίκαιρο, αποτελεσματικό και προσαρμοσμένο στις εξελισσόμενες απειλές και κινδύνους.

Συνολικά, οι ανεξάρτητοι έλεγχοι λειτουργούν ως εργαλείο λογοδοσίας, διαφάνειας και συνεχούς βελτίωσης, ενισχύοντας τη θεσμική αξιοπιστία των βασικών οντοτήτων και τη συμμόρφωσή τους με τις σύγχρονες κανονιστικές απαιτήσεις στον τομέα της κυβερνοασφάλειας.

6.2.3 Διαδικασίες παρακολούθησης της συμμόρφωσης

Η παρακολούθηση και η αξιολόγηση της συμμόρφωσης των βασικών και σημαντικών οντοτήτων με τις κανονιστικές τους υποχρεώσεις στον τομέα της κυβερνοασφάλειας αποτελούν αναπόσπαστο στοιχείο της οργανωτικής διακυβέρνησης και της αποτελεσματικής διαχείρισης κινδύνων. Στο πλαίσιο αυτό, οι οντότητες οφείλουν να υλοποιούν συστηματικές διαδικασίες ελέγχου της συμμόρφωσής τους προς το ισχύον εθνικό και ενωσιακό κανονιστικό πλαίσιο, διασφαλίζοντας ότι οι πολιτικές, οι διαδικασίες και τα τεχνικά μέτρα που εφαρμόζονται ανταποκρίνονται στις προβλεπόμενες απαιτήσεις κυβερνοασφάλειας.

Τα αποτελέσματα των διαδικασιών παρακολούθησης και αξιολόγησης αποτυπώνονται σε σχετικές αναφορές, οι οποίες υποβάλλονται σε τακτική βάση στο ανώτατο όργανο διοίκησης της οντότητας. Η ενημέρωση αυτή ενισχύει τη λογοδοσία σε ανώτατο διοικητικό επίπεδο και επιτρέπει τη λήψη τεκμηριωμένων αποφάσεων αναφορικά με την ενίσχυση ή την αναθεώρηση των εφαρμοζόμενων μέτρων ασφάλειας.

Σε περίπτωση που από την αξιολόγηση προκύψει μη συμμόρφωση της οντότητας με τις κανονιστικές της υποχρεώσεις, ενεργοποιείται η ευθύνη του ανώτατου οργάνου διοίκησης, το οποίο υποχρεούται να εκκινήσει διαδικασίες λήψης διορθωτικών ενεργειών. Οι ενέργειες αυτές αποσκοπούν στην άρση των διαπιστωθεισών αποκλίσεων, στη μείωση των σχετικών κινδύνων και στην αποκατάσταση της συμμόρφωσης εντός εύλογου χρονικού διαστήματος.

Οι διαδικασίες παρακολούθησης και αξιολόγησης της συμμόρφωσης διενεργούνται σε προγραμματισμένα χρονικά διαστήματα, στο πλαίσιο ενός κύκλου συνεχούς βελτίωσης, αλλά και εκτάκτως, όταν επέρχονται μεταβολές στο κανονιστικό περιβάλλον ή σημαντικές αλλαγές στις λειτουργίες, στις υποδομές ή στο επιχειρησιακό μοντέλο της οντότητας. Η δυναμική αυτή προσέγγιση διασφαλίζει ότι η συμμόρφωση παραμένει επίκαιρη και αποτελεσματική, ανταποκρινόμενη στις εξελισσόμενες νομικές απαιτήσεις και στις μεταβαλλόμενες απειλές του κυβερνοχώρου.

Συνολικά, η συστηματική παρακολούθηση της συμμόρφωσης λειτουργεί ως βασικός μηχανισμός πρόληψης, ελέγχου και θεσμικής θωράκισης των βασικών και σημαντικών οντοτήτων, ενισχύοντας τη διαφάνεια, τη διοικητική υπευθυνότητα και τη συνολική ανθεκτικότητα στον τομέα της κυβερνοασφάλειας.

6.2.4 Ασφάλεια ανθρώπινου δυναμικού

Η διαχείριση του ανθρώπινου δυναμικού συνιστά κρίσιμο παράγοντα για την αποτελεσματική εφαρμογή των μέτρων κυβερνοασφάλειας από τις βασικές και σημαντικές οντότητες, καθώς ο ανθρώπινος παράγοντας δύναται να λειτουργήσει τόσο ως στοιχείο ενίσχυσης όσο και ως πηγή κινδύνου για την ασφάλεια των πληροφοριακών συστημάτων. Στο πλαίσιο αυτό, οι οντότητες οφείλουν να υλοποιούν κατάλληλες διαδικασίες ελέγχου καταλληλότητας του υποψηφίου προσωπικού, με στόχο τη διασφάλιση ότι τα άτομα που εντάσσονται στον οργανισμό πληρούν τα απαιτούμενα κριτήρια αξιοπιστίας και επαγγελματικής επάρκειας.

Περαιτέρω, ιδιαίτερη σημασία αποδίδεται στον σαφή καθορισμό και στην έγκαιρη κοινοποίηση προς το αρμόδιο προσωπικό των ευθυνών και των υποχρεώσεων που εξακολουθούν να ισχύουν μετά τη λήξη της εργασιακής σχέσης ή σε περίπτωση μεταβολής της κατάστασης απασχόλησης. Η ρύθμιση αυτή αποσκοπεί στη διασφάλιση της συνέχειας της προστασίας των πληροφοριών και των συστημάτων, ιδίως ως προς την εμπιστευτικότητα και την αποφυγή μη εξουσιοδοτημένης χρήσης ή γνωστοποίησης δεδομένων.

Παράλληλα, οι οντότητες ορίζουν και εφαρμόζουν διαδικασίες πειθαρχικού ελέγχου για περιπτώσεις παραβίασης της γενικής πολιτικής ασφάλειας πληροφοριών ή

των επιμέρους θεματικών πολιτικών ασφάλειας. Οι διαδικασίες αυτές λειτουργούν αποτρεπτικά, ενισχύουν την υπευθυνότητα του προσωπικού και συμβάλλουν στη δημιουργία κουλτούρας συμμόρφωσης και ασφάλειας εντός του οργανισμού.

Ειδικότερα για τις βασικές οντότητες, προβλέπεται η εφαρμογή επιπρόσθετων μέτρων, όπως οι διαδικασίες επαλήθευσης του ιστορικού του υποψηφίου προσωπικού (background checks), καθώς και, κατά περίπτωση, η αξιολόγηση ζητημάτων αμεροληψίας και ακεραιότητας. Τα μέτρα αυτά αφορούν ιδίως το προσωπικό που πρόκειται να αναλάβει ρόλους και αρμοδιότητες συναφείς με την κυβερνοασφάλεια και αποσκοπούν στην επιβεβαίωση της διαρκούς καταλληλότητάς του, τόσο ως προς τις τεχνικές και επαγγελματικές του ικανότητες όσο και ως προς την αξιοπιστία και την ηθική του συγκρότηση.

Συνολικά, οι ανωτέρω διαδικασίες αναδεικνύουν τη σημασία μιας ολοκληρωμένης προσέγγισης στη διαχείριση του ανθρώπινου δυναμικού, στο πλαίσιο της οποίας η κυβερνοασφάλεια δεν αντιμετωπίζεται αποκλειστικά ως τεχνικό ζήτημα, αλλά ως οργανωτική και θεσμική πρόκληση που απαιτεί συνεχή έλεγχο, υπευθυνότητα και επαγρύπνηση.

6.2.5 Διαχείριση υλικού και λογισμικού

Η συστηματική διαχείριση των αγαθών πληροφορικής και των δεδομένων αποτελεί βασικό στοιχείο της οργανωτικής και τεχνικής θωράκισης των βασικών και σημαντικών οντοτήτων έναντι κινδύνων κυβερνοασφάλειας. Στο πλαίσιο αυτό, οι οντότητες οφείλουν να τηρούν ακριβή, πλήρη και διαρκώς επικαιροποιημένο κατάλογο των αγαθών πληροφορικής που διαθέτουν ή διαχειρίζονται, συμπεριλαμβανομένου του υλικού, του λογισμικού, των πληροφοριακών συστημάτων, των κατηγοριών δεδομένων και των παρεχόμενων υπηρεσιών. Ο κατάλογος αυτός καλύπτει τόσο τα αγαθά που φιλοξενούνται στις φυσικές εγκαταστάσεις της οντότητας όσο και εκείνα που λειτουργούν σε περιβάλλοντα νεφοϋπολογιστικής (cloud), ενώ περιλαμβάνει, όπου υφίστανται, και αγαθά επιχειρησιακής τεχνολογίας (operational technology – OT), τα οποία συχνά χαρακτηρίζονται από αυξημένη κρισιμότητα.

Για κάθε επιμέρους αγαθό, η οντότητα ορίζει ρητώς έναν υπεύθυνο ιδιοκτήτη (asset owner), ο οποίος αναλαμβάνει τη συνολική ευθύνη για τη διαχείριση, τη συντήρηση και την ασφάλειά του καθ' όλη τη διάρκεια του κύκλου ζωής του. Η σαφής απόδοση αρμοδιοτήτων συμβάλλει στη λογοδοσία και στη βελτιωμένη αντιμετώπιση κινδύνων που συνδέονται με την απώλεια, την αλλοίωση ή τη μη εξουσιοδοτημένη χρήση των αγαθών.

Παράλληλα, οι βασικές και σημαντικές οντότητες εφαρμόζουν διαδικασίες ταξινόμησης των δεδομένων και των αγαθών σε διακριτά επίπεδα, βάσει των απαιτήσεων εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας. Η αντιστοίχιση κάθε αγαθού και συνόλου δεδομένων σε συγκεκριμένο επίπεδο ταξινόμησης πραγματοποιείται με γνώμονα την ευαισθησία, την επιχειρησιακή κρισιμότητα και τη συνολική αξία τους για την οντότητα, επιτρέποντας την αναλογική εφαρμογή μέτρων προστασίας.

Επιπροσθέτως, η οντότητα εκπονεί γραπτή πολιτική και αναλυτικές οδηγίες για την ορθή χρήση των αγαθών και των δεδομένων καθ' όλη τη διάρκεια του κύκλου ζωής τους. Οι ρυθμίσεις αυτές καλύπτουν όλα τα στάδια, από την προμήθεια και την καθημερινή χρήση έως την αποθήκευση, τη μεταφορά και την ασφαλή απομάκρυνση ή διαγραφή τους, διασφαλίζοντας ότι η διαχείριση πραγματοποιείται με τρόπο συμβατό με τις αρχές της κυβερνοασφάλειας και της κανονιστικής συμμόρφωσης.

Τέλος, ιδιαίτερη έμφαση αποδίδεται στη διαχείριση των αφαιρούμενων μέσων αποθήκευσης, για τα οποία η οντότητα οφείλει να θεσπίζει ειδική γραπτή πολιτική ασφαλούς χρήσης και χειρισμού. Η πολιτική αυτή ευθυγραμμίζεται με το σχήμα ταξινόμησης των αγαθών και των δεδομένων και αποσκοπεί στον περιορισμό κινδύνων που σχετίζονται με απώλεια, διαρροή ή κακόβουλη εκμετάλλευση πληροφοριών.

Συνολικά, η ολοκληρωμένη διαχείριση αγαθών και δεδομένων συνιστά θεμελιώδη προϋπόθεση για την αποτελεσματική εφαρμογή των μέτρων κυβερνοασφάλειας, καθώς παρέχει τη βάση για την ορθή αξιολόγηση κινδύνων, την αναλογική κατανομή πόρων και τη διασφάλιση της επιχειρησιακής συνέχειας των βασικών και σημαντικών οντοτήτων.

6.2.6 Διαχείριση λογαριασμών και έλεγχος πρόσβασης

Ο λογικός έλεγχος πρόσβασης στα συστήματα δικτύου και πληροφοριών αποτελεί θεμελιώδη συνιστώσα της κυβερνοασφάλειας των βασικών και σημαντικών οντοτήτων, καθώς διασφαλίζει ότι η πρόσβαση σε κρίσιμα πληροφοριακά αγαθά παρέχεται αποκλειστικά σε εξουσιοδοτημένα πρόσωπα και συστήματα, σύμφωνα με τις επιχειρησιακές ανάγκες και τις απαιτήσεις ασφάλειας. Στο πλαίσιο αυτό, οι οντότητες οφείλουν να εκπονούν και να εφαρμόζουν σαφείς πολιτικές και διαδικασίες λογικού ελέγχου πρόσβασης, οι οποίες καθορίζουν τους κανόνες, τα δικαιώματα και τους περιορισμούς πρόσβασης στα συστήματα δικτύου και πληροφοριών τους.

Οι πολιτικές αυτές λαμβάνουν υπόψη τόσο τις επιχειρηματικές ανάγκες της οντότητας όσο και τις ειδικές αρμοδιότητές της, ιδίως όταν πρόκειται για οντότητες που υπάγονται σε ειδικές κατηγορίες του εφαρμοστέου νομοθετικού πλαισίου. Παράλληλα, καλύπτουν το σύνολο των χρηστών που αποκτούν πρόσβαση στα συστήματα, συμπεριλαμβανομένου του εσωτερικού προσωπικού, αλλά και προσωπικού τρίτων οντοτήτων, όπως προμηθευτών και παρόχων υπηρεσιών Τεχνολογιών Πληροφορικής και Επικοινωνιών. Με τον τρόπο αυτό, διασφαλίζεται ενιαία και συνεκτική αντιμετώπιση των κινδύνων που σχετίζονται με την πρόσβαση τρίτων σε κρίσιμες υποδομές και δεδομένα.

Κεντρικό στοιχείο του πλαισίου λογικού ελέγχου πρόσβασης αποτελεί η χορήγηση μοναδικής ταυτότητας (identity) σε κάθε χρήστη και σε κάθε σύστημα που αποκτά πρόσβαση στα συστήματα δικτύου και πληροφοριών της οντότητας. Η πρακτική αυτή επιτρέπει την ακριβή ταυτοποίηση των ενεργειών που εκτελούνται, ενισχύοντας τη λογοδοσία και τη δυνατότητα ιχνηλασιμότητας σε περίπτωση περιστατικών ασφάλειας ή παραβίασης πολιτικών. Η μοναδικότητα της ταυτότητας συνιστά προϋπόθεση για την αποτελεσματική εφαρμογή μηχανισμών ελέγχου, καταγραφής και ελέγχου συμμόρφωσης.

Συνολικά, η θέσπιση και η συνεπής εφαρμογή πολιτικών λογικού ελέγχου πρόσβασης συμβάλλει καθοριστικά στον περιορισμό της μη εξουσιοδοτημένης πρόσβασης, στη μείωση του κινδύνου κατάχρησης δικαιωμάτων και στην ενίσχυση της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των πληροφοριών.

Παράλληλα, ενδυναμώνει τη θεσμική λογοδοσία και την οργανωτική ωριμότητα των βασικών και σημαντικών οντοτήτων στο σύγχρονο ψηφιακό περιβάλλον.

6.2.7 Ασφαλής παραμετροποίηση υλικού, λογισμικού, υπηρεσιών και δικτύων

Η ασφαλής παραμετροποίηση των πληροφοριακών συστημάτων και υποδομών αποτελεί θεμελιώδη οργανωτικό και τεχνικό μέτρο κυβερνοασφάλειας για τις βασικές και σημαντικές οντότητες, καθώς επηρεάζει άμεσα το επίπεδο έκθεσής τους σε απειλές και ευπάθειες. Στο πλαίσιο αυτό, οι οντότητες οφείλουν να αναπτύσσουν και να εφαρμόζουν συστηματικές διαδικασίες και κατάλληλα εργαλεία για την επιβολή ελεγχόμενων ρυθμίσεων και παραμετροποιήσεων στο υλικό, στο λογισμικό, στις παρεχόμενες υπηρεσίες και στο δίκτυό τους, συμπεριλαμβανομένων των κρίσιμων ρυθμίσεων ασφάλειας.

Η ύπαρξη τυποποιημένων και τεκμηριωμένων ρυθμίσεων συμβάλλει στη διασφάλιση της ομοιομορφίας, της προβλεψιμότητας και της επαναληψιμότητας των μέτρων ασφάλειας, περιορίζοντας τα σφάλματα που οφείλονται σε αυθαίρετες ή μη ελεγχόμενες παραμετροποιήσεις. Παράλληλα, επιτρέπει τον αποτελεσματικό έλεγχο συμμόρφωσης και τη γρήγορη αποκατάσταση των συστημάτων σε περίπτωση περιστατικού ή αστοχίας.

Ειδικότερα, οι βασικές και σημαντικές οντότητες εφαρμόζουν διαδικασίες ασφαλούς παραμετροποίησης (secure configuration) για το σύνολο του τεχνολογικού τους περιβάλλοντος, καλύπτοντας τόσο τις αρχικές ρυθμίσεις όσο και τις μεταγενέστερες αλλαγές κατά τη λειτουργία των συστημάτων. Στο πλαίσιο αυτό, δύνανται να αξιοποιούνται προκαθορισμένα πρότυπα και κατευθυντήριες οδηγίες κατασκευαστών, καθώς και πρότυπα ή συστάσεις ανεξάρτητων ερευνητικών και θεσμικών οργανισμών, τα οποία ενσωματώνουν βέλτιστες πρακτικές κυβερνοασφάλειας.

Παράλληλα, η ασφαλής παραμετροποίηση βασίζεται στην εφαρμογή θεμελιωδών αρχών κυβερνοασφάλειας, όπως η αρχή της «ελάχιστης λειτουργικότητας» (least functionality), σύμφωνα με την οποία ενεργοποιούνται μόνο οι απολύτως αναγκαίες λειτουργίες και υπηρεσίες, και η αρχή των «ελάχιστων προνομίων» (least privilege), βάσει της οποίας οι χρήστες και τα συστήματα διαθέτουν αποκλειστικά τα

δικαιώματα που απαιτούνται για την εκτέλεση των αρμοδιοτήτων τους. Οι αρχές αυτές συμβάλλουν ουσιαστικά στη μείωση της επιφάνειας επίθεσης και στον περιορισμό των συνεπειών ενδεχόμενης παραβίασης.

Συνολικά, η υιοθέτηση και η συνεπής εφαρμογή διαδικασιών ασφαλούς παραμετροποίησης ενισχύει τη λειτουργική ανθεκτικότητα των βασικών και σημαντικών οντοτήτων, μειώνει τον κίνδυνο εκμετάλλευσης γνωστών ή άγνωστων ευπαθειών και αποτελεί αναγκαία προϋπόθεση για την αποτελεσματική και βιώσιμη προστασία των συστημάτων δικτύου και πληροφοριών στο σύγχρονο ψηφιακό περιβάλλον.

6.2.8 Αρχές ασφαλούς ανάπτυξης εφαρμογών

Η ασφάλεια των εφαρμογών συνιστά κρίσιμο παράγοντα για τη συνολική στάθμη κυβερνοασφάλειας των βασικών και σημαντικών οντοτήτων, ιδίως δεδομένου ότι οι εφαρμογές αποτελούν βασικό σημείο αλληλεπίδρασης μεταξύ χρηστών, δεδομένων και πληροφοριακών συστημάτων. Στο πλαίσιο αυτό, οι οντότητες οφείλουν να ενσωματώνουν τις απαιτήσεις ασφάλειας ήδη από τα πρώιμα στάδια του κύκλου ζωής των εφαρμογών, ήτοι κατά τον σχεδιασμό και τη διαμόρφωση των λειτουργικών και τεχνικών προδιαγραφών τους. Οι απαιτήσεις αυτές καθορίζονται με βάση την κρισιμότητα κάθε εφαρμογής, τον ρόλο της στις επιχειρησιακές διαδικασίες και τους κινδύνους που απορρέουν από τη λειτουργία, τη διασύνδεση και τη διαχείριση των δεδομένων της.

Περαιτέρω, οι βασικές και σημαντικές οντότητες διασφαλίζουν ότι οι εφαρμογές που αποκτούν ή αναπτύσσουν συμμορφώνονται με καθιερωμένες αρχές συγγραφής ασφαλούς κώδικα και σχεδίασης ασφαλούς αρχιτεκτονικής. Ιδιαίτερη σημασία αποδίδεται στην εφαρμογή της αρχής της «ασφάλειας από το σχεδιασμό» (security by design), σύμφωνα με την οποία η ασφάλεια ενσωματώνεται εξαρχής στη δομή και στη λειτουργικότητα της εφαρμογής και δεν προστίθεται εκ των υστέρων ως συμπληρωματικό μέτρο. Παράλληλα, η αρχή της «ασφάλειας εξ ορισμού» (security by default) διασφαλίζει ότι οι προεπιλεγμένες ρυθμίσεις των εφαρμογών παρέχουν το υψηλότερο δυνατό επίπεδο προστασίας, περιορίζοντας την ανάγκη χειροκίνητων παρεμβάσεων από τους χρήστες.

Επιπλέον, η αρχή των «ελάχιστων προνομίων» (least privilege) εφαρμόζεται τόσο σε επίπεδο χρηστών όσο και σε επίπεδο εφαρμογών και υπηρεσιών, εξασφαλίζοντας ότι η πρόσβαση σε λειτουργίες και δεδομένα περιορίζεται αποκλειστικά στο απολύτως αναγκαίο για την εκτέλεση συγκεκριμένων καθηκόντων. Η προσέγγιση αυτή συμπληρώνεται από την αρχή της «μηδενικής εμπιστοσύνης» (zero-trust), σύμφωνα με την οποία καμία οντότητα, χρήστης ή σύστημα δεν θεωρείται εξ ορισμού αξιόπιστο, ανεξαρτήτως της θέσης του εντός ή εκτός του οργανωτικού περιβάλλοντος, και κάθε αίτημα πρόσβασης υπόκειται σε συνεχή έλεγχο και επαλήθευση.

Συνολικά, η ενσωμάτωση των αρχών αυτών στον σχεδιασμό, την ανάπτυξη και την προμήθεια εφαρμογών ενισχύει ουσιαστικά την ανθεκτικότητα των πληροφοριακών συστημάτων, μειώνει την πιθανότητα εκμετάλλευσης ευπαθειών και συμβάλλει στη δημιουργία ενός ώριμου και βιώσιμου πλαισίου κυβερνοασφάλειας. Με τον τρόπο αυτό, οι βασικές και σημαντικές οντότητες αντιμετωπίζουν την ασφάλεια εφαρμογών όχι ως αποσπασματική τεχνική απαίτηση, αλλά ως οργανικό και διαρκές στοιχείο της ψηφιακής τους διακυβέρνησης.

6.2.9 Αξιολόγηση της αποτελεσματικότητας των μέτρων διαχείρισης κινδύνων κυβερνοασφάλειας

Οι έλεγχοι κυβερνοασφάλειας αποτελούν ουσιώδες εργαλείο για την αξιολόγηση της αποτελεσματικότητας των μέτρων διαχείρισης κινδύνων που εφαρμόζουν οι βασικές και σημαντικές οντότητες στα συστήματα δικτύου και πληροφοριών τους. Στο πλαίσιο αυτό, οι οντότητες οφείλουν να εκπονούν και να εφαρμόζουν σαφώς καθορισμένη πολιτική και διαδικασίες που διέπουν τη διενέργεια ελέγχων κυβερνοασφάλειας, με σκοπό τη συστηματική αποτίμηση της επάρκειας και της αποδοτικότητας των οργανωτικών, τεχνικών και επιχειρησιακών μέτρων που έχουν υλοποιηθεί.

Οι εν λόγω πολιτικές και διαδικασίες προσδιορίζουν, κατ' ελάχιστον, το πεδίο εφαρμογής των ελέγχων, τη συχνότητά τους και το είδος των δοκιμών που πραγματοποιούνται, λαμβάνοντας υπόψη την κρισιμότητα των συστημάτων, την πολυπλοκότητα των υποδομών και το επίπεδο των υφιστάμενων απειλών. Η τυποποιημένη αυτή προσέγγιση διασφαλίζει τη συνέπεια και τη συγκρισιμότητα των

αποτελεσμάτων των ελέγχων, ενώ παράλληλα διευκολύνει την παρακολούθηση της προόδου και τη λήψη διορθωτικών μέτρων.

Ιδιαίτερη σημασία αποδίδεται στη διενέργεια εξωτερικών ελέγχων παρείσδυσης (external penetration tests), οι οποίοι πραγματοποιούνται σε περιοδική βάση και, σε κάθε περίπτωση, τουλάχιστον μία φορά ετησίως. Επιπλέον, οι έλεγχοι αυτοί ενεργοποιούνται εκτάκτως μετά την εκδήλωση σοβαρού περιστατικού κυβερνοασφάλειας, προκειμένου να αξιολογηθεί το εύρος των αδυναμιών που εκμεταλλεύτηκε το περιστατικό και να εντοπιστούν τυχόν πρόσθετες ευπάθειες. Η ανάθεση των ελέγχων παρείσδυσης σε εξωτερικούς, εξειδικευμένους φορείς ενισχύει την αντικειμενικότητα της αξιολόγησης και παρέχει ανεξάρτητη εικόνα της πραγματικής ανθεκτικότητας των συστημάτων έναντι επιθέσεων.

Συνολικά, η θεσμοθέτηση και η τακτική διενέργεια ελέγχων κυβερνοασφάλειας και εξωτερικών δοκιμών παρείσδυσης ενισχύει τη συνεχή βελτίωση του επιπέδου ασφάλειας των βασικών και σημαντικών οντοτήτων. Παράλληλα, συμβάλλει στην έγκαιρη αναγνώριση αδυναμιών, στη μείωση της επιφάνειας επίθεσης και στη διασφάλιση της συμμόρφωσης με τις σύγχρονες κανονιστικές και επιχειρησιακές απαιτήσεις στον τομέα της κυβερνοασφάλειας.

6.2.10 Ασφάλεια δικτύων

Η ασφάλεια των δικτύων και των δικτυακών υποδομών αποτελεί θεμελιώδη προϋπόθεση για τη διασφάλιση της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των πληροφοριακών συστημάτων των βασικών και σημαντικών οντοτήτων. Στο πλαίσιο αυτό, οι οντότητες οφείλουν να εκπονούν και να εφαρμόζουν γραπτή πολιτική και τεκμηριωμένες διαδικασίες που αφορούν στην προστασία των δικτύων και των δικτυακών συσκευών τους από μη εξουσιοδοτημένη πρόσβαση, κακόβουλες ενέργειες και παραβιάσεις ασφάλειας.

Κεντρικό ρόλο στο πλαίσιο προστασίας των δικτύων διαδραματίζει η υλοποίηση κατάλληλων τεχνικών μέτρων ελέγχου της δικτυακής κυκλοφορίας. Ειδικότερα, οι βασικές και σημαντικές οντότητες εφαρμόζουν τείχη προστασίας (firewalls), τα οποία λειτουργούν ως βασικός μηχανισμός περιορισμού και φιλτραρίσματος των εισερχόμενων

και εξερχόμενων δικτυακών συνδέσεων, αποτρέποντας τη μη εξουσιοδοτημένη πρόσβαση στο εσωτερικό δίκτυο. Η παραμετροποίηση και η λειτουργία των τειχών προστασίας προσαρμόζονται στο επίπεδο επικινδυνότητας και στην κρισιμότητα των επιμέρους υποδικτύων ή ζωνών ασφαλείας, λαμβάνοντας υπόψη την αρχή της αναλογικότητας.

Σε περιβάλλοντα αυξημένης κρισιμότητας ή έκθεσης σε κυβερνοαπειλές, οι οντότητες δύνανται να υλοποιούν επιπρόσθετα προηγμένες τεχνολογίες ασφάλειας, όπως συστήματα ανίχνευσης ή πρόληψης εισβολών (intrusion detection systems – IDS και intrusion prevention systems – IPS), καθώς και τείχη προστασίας εφαρμογών ιστού (web application firewalls – WAF). Οι τεχνολογίες αυτές ενισχύουν τη δυνατότητα έγκαιρης ανίχνευσης και απόκρισης σε κακόβουλες δραστηριότητες, προσφέροντας πολυεπίπεδη άμυνα στο δικτυακό περιβάλλον.

Παράλληλα, οι βασικές και σημαντικές οντότητες θεσπίζουν και εφαρμόζουν κανόνες που αφορούν στην ασφαλή σύνδεση στο δίκτυο, στις απαιτήσεις αυθεντικοποίησης των χρηστών και των συστημάτων, καθώς και στις διαδικασίες εξουσιοδότησης πρόσβασης στις δικτυακές υπηρεσίες. Οι κανόνες αυτοί αποσκοπούν στον έλεγχο και στον περιορισμό της πρόσβασης αποκλειστικά σε εξουσιοδοτημένα πρόσωπα και συστήματα, μειώνοντας τον κίνδυνο κατάχρησης δικαιωμάτων και μη εξουσιοδοτημένων ενεργειών.

Συνολικά, η υιοθέτηση ολοκληρωμένων πολιτικών και τεχνικών μέτρων προστασίας δικτύων ενισχύει ουσιαστικά την ανθεκτικότητα των βασικών και σημαντικών οντοτήτων απέναντι σε κυβερνοαπειλές, περιορίζει την επιφάνεια επίθεσης και συμβάλλει στη διασφάλιση της απρόσκοπτης και ασφαλούς λειτουργίας των δικτυακών και πληροφοριακών τους υποδομών.

6.2.11 Προστασία από κακόβουλο λογισμικό

Η προστασία των πληροφοριακών συστημάτων από κακόβουλο λογισμικό και μη εξουσιοδοτημένη εκτέλεση εφαρμογών αποτελεί θεμελιώδη τεχνικό και οργανωτικό μέτρο στο πλαίσιο διαχείρισης κινδύνων κυβερνοασφάλειας των βασικών και σημαντικών οντοτήτων, όπως αυτό προβλέπεται από την Οδηγία (ΕΕ) 2022/2555 (NIS2)

και τον εφαρμοστικό ν. 5160/2024. Οι σύγχρονες κυβερνοαπειλές χαρακτηρίζονται από αυξημένη πολυπλοκότητα, αυτοματοποίηση και δυνατότητα ταχείας εξάπλωσης, γεγονός που καθιστά αναγκαία την υιοθέτηση πολυεπίπεδων μηχανισμών πρόληψης, ανίχνευσης και απόκρισης.

Στο πλαίσιο αυτό, οι βασικές και σημαντικές οντότητες οφείλουν να υλοποιούν σε σταθμούς εργασίας, διακομιστές και δικτυακές συσκευές κατάλληλες τεχνολογίες ανίχνευσης και εξουδετέρωσης κακόβουλου λογισμικού. Οι τεχνολογίες αυτές περιλαμβάνουν, ενδεικτικά, λύσεις antivirus, anti-malware, endpoint detection and response (EDR) και, κατά περίπτωση, extended detection and response (XDR), οι οποίες επιτρέπουν τη συνεχή παρακολούθηση της συμπεριφοράς των συστημάτων και την έγκαιρη αναγνώριση ύποπτων ή κακόβουλων ενεργειών. Η εφαρμογή των εν λόγω τεχνολογιών δεν περιορίζεται μόνο στην προστασία των τελικών χρηστών, αλλά επεκτείνεται στο σύνολο της υποδομής, συμπεριλαμβανομένων κρίσιμων διακομιστών και δικτυακών στοιχείων.

Ιδιαίτερη σημασία αποδίδεται στην αυτοματοποιημένη εγκατάσταση και ενημέρωση των μηχανισμών προστασίας. Η αυτοματοποίηση των ενημερώσεων διασφαλίζει ότι οι τεχνολογίες ανίχνευσης κακόβουλου λογισμικού παραμένουν διαρκώς επικαιροποιημένες έναντι νέων απειλών και ευπαθειών, περιορίζοντας τον κίνδυνο εκμετάλλευσης γνωστών κενών ασφαλείας. Η προσέγγιση αυτή ευθυγραμμίζεται με τη λογική της NIS2, η οποία απαιτεί από τις οντότητες να υιοθετούν μέτρα που διασφαλίζουν την επιχειρησιακή συνέχεια και την ανθεκτικότητα των συστημάτων δικτύου και πληροφοριών.

Παράλληλα με την ανίχνευση κακόβουλου λογισμικού, οι βασικές και σημαντικές οντότητες υποχρεούνται να υλοποιούν κανόνες και τεχνολογίες ελέγχου της εκτέλεσης εφαρμογών. Οι μηχανισμοί αυτοί αποσκοπούν στον περιορισμό της εκτέλεσης μη εξουσιοδοτημένου ή δυνητικά επικίνδυνου λογισμικού σε σταθμούς εργασίας, διακομιστές και δικτυακές συσκευές. Τέτοιες τεχνολογίες περιλαμβάνουν, μεταξύ άλλων, application whitelisting και blacklisting, έλεγχο ψηφιακών υπογραφών, πολιτικές περιορισμού εφαρμογών και μηχανισμούς sandboxing.

Ο έλεγχος εκτέλεσης εφαρμογών λειτουργεί συμπληρωματικά προς τις παραδοσιακές λύσεις antivirus, καθώς επιτρέπει την πρόληψη απειλών ακόμη και σε

περιπτώσεις όπου το κακόβουλο λογισμικό δεν έχει ακόμη αναγνωριστεί από βάσεις δεδομένων υπογραφών. Με τον τρόπο αυτό, μειώνεται σημαντικά η επιφάνεια επίθεσης και περιορίζεται η δυνατότητα εκτέλεσης κακόβουλων κώδικων που εκμεταλλεύονται ανθρώπινα σφάλματα ή τεχνικές κοινωνικής μηχανικής.

Η εφαρμογή των ανωτέρω μέτρων πρέπει να εντάσσεται σε ένα συνολικό πλαίσιο πολιτικών και διαδικασιών κυβερνοασφάλειας, το οποίο εγκρίνεται και εποπτεύεται από το ανώτατο όργανο διοίκησης της οντότητας, σύμφωνα με τις απαιτήσεις διακυβέρνησης της NIS2. Η αποτελεσματικότητα των τεχνολογιών προστασίας αξιολογείται μέσω τακτικών ελέγχων, δοκιμών και επαναξιολογήσεων, ενώ τα ευρήματα τροφοδοτούν διαδικασίες συνεχούς βελτίωσης.

Επιπλέον, η επιτυχής εφαρμογή των τεχνολογικών μέτρων προϋποθέτει την κατάλληλη εκπαίδευση και ευαισθητοποίηση του προσωπικού. Οι χρήστες των συστημάτων καλούνται να κατανοούν τις βασικές αρχές ασφαλούς χρήσης εφαρμογών και να συμμορφώνονται με τις πολιτικές της οντότητας, συμβάλλοντας ενεργά στην πρόληψη περιστατικών κυβερνοασφάλειας.

Συνολικά, η υλοποίηση τεχνολογιών ανίχνευσης και εξουδετέρωσης κακόβουλου λογισμικού, σε συνδυασμό με τον έλεγχο εκτέλεσης εφαρμογών, αποτελεί κρίσιμο μέτρο συμμόρφωσης με την Οδηγία NIS2 και τον ν. 5160/2024. Τα μέτρα αυτά ενισχύουν την ανθεκτικότητα των βασικών και σημαντικών οντοτήτων, περιορίζουν την πιθανότητα και τον αντίκτυπο κυβερνοεπιθέσεων και συμβάλλουν στη διασφάλιση της αξιοπιστίας και της ασφάλειας των παρεχόμενων υπηρεσιών σε ένα διαρκώς μεταβαλλόμενο ψηφιακό περιβάλλον.

6.2.12 Χρήση κρυπτογραφίας

Η κρυπτογραφία αποτελεί θεμελιώδες τεχνικό και οργανωτικό μέτρο για την προστασία των δεδομένων και των πληροφοριακών συστημάτων των βασικών και σημαντικών οντοτήτων, ιδίως σε περιβάλλοντα αυξημένου ψηφιακού κινδύνου. Στο πλαίσιο αυτό, οι οντότητες οφείλουν να εκπονούν και να εφαρμόζουν γραπτή πολιτική και τεκμηριωμένες διαδικασίες που αφορούν στη χρήση κρυπτογραφικών μηχανισμών, με σκοπό τη διασφάλιση της εμπιστευτικότητας, της ακεραιότητας και της

αυθεντικότητας των δεδομένων που διαχειρίζονται. Η πολιτική αυτή οφείλει να ευθυγραμμίζεται τόσο με το εσωτερικό σχήμα ταξινόμησης των αγαθών και των δεδομένων όσο και με τα αποτελέσματα της αποτίμησης επικινδυνότητας, υιοθετώντας μια προσέγγιση βασισμένη στον κίνδυνο (risk-based approach).

Η απαίτηση αυτή απορρέει άμεσα από το άρθρο 32 του ΓΚΠΔ, το οποίο επιβάλλει στους υπευθύνους επεξεργασίας και στους εκτελούντες την επεξεργασία την υποχρέωση εφαρμογής κατάλληλων τεχνικών και οργανωτικών μέτρων, λαμβάνοντας υπόψη τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας, καθώς και τους κινδύνους διαφορετικής πιθανότητας και σοβαρότητας για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων. Στο ίδιο άρθρο, η κρυπτογράφηση αναγνωρίζεται ρητώς ως ενδεικτικό μέτρο για την ενίσχυση της ασφάλειας της επεξεργασίας.

Στο πλαίσιο αυτό, η πολιτική κρυπτογραφίας της οντότητας καθορίζει, μεταξύ άλλων, τους τύπους δεδομένων που υπόκεινται σε κρυπτογράφηση, τα αποδεκτά κρυπτογραφικά πρότυπα και αλγορίθμους, τις διαδικασίες διαχείρισης και προστασίας των κλειδιών κρυπτογράφησης, καθώς και τις ευθύνες των εμπλεκόμενων ρόλων. Ιδιαίτερη σημασία αποδίδεται στη διασφάλιση ότι οι χρησιμοποιούμενοι κρυπτογραφικοί μηχανισμοί είναι σύγχρονοι, αξιόπιστοι και σύμφωνοι με διεθνώς αναγνωρισμένα πρότυπα, ώστε να αποτρέπεται η υποβάθμιση της ασφάλειας λόγω τεχνολογικής απαξίωσης.

Παράλληλα, οι βασικές και σημαντικές οντότητες οφείλουν να διασφαλίζουν ότι τα δεδομένα που έχουν ταξινομηθεί ως αυξημένης κρισιμότητας κρυπτογραφούνται κατά την αποθήκευσή τους (encryption at rest). Η απαίτηση αυτή αφορά δεδομένα που είναι αποθηκευμένα σε υπολογιστές τελικού χρήστη, διακομιστές, αφαιρούμενα μέσα αποθήκευσης, εφαρμογές και βάσεις δεδομένων, ανεξαρτήτως του αν αυτά βρίσκονται σε τοπικές υποδομές ή σε περιβάλλοντα νεφοϋπολογιστικής. Η κρυπτογράφηση σε κατάσταση αδράνειας αποσκοπεί στον περιορισμό του κινδύνου μη εξουσιοδοτημένης πρόσβασης σε περίπτωση απώλειας, κλοπής ή παραβίασης συσκευών και συστημάτων.

Η εφαρμογή της κρυπτογράφησης at rest ενισχύει ουσιωδώς την προστασία των δεδομένων προσωπικού χαρακτήρα, καθώς ακόμη και σε περίπτωση παραβίασης της ασφάλειας, τα δεδομένα καθίστανται πρακτικά μη αναγνώσιμα για μη εξουσιοδοτημένα πρόσωπα. Στο πλαίσιο του ΓΚΠΔ, το στοιχείο αυτό μπορεί να λειτουργήσει και ως

παράγοντας μετριασμού του κινδύνου για τα δικαιώματα των υποκειμένων των δεδομένων, επηρεάζοντας, κατά περίπτωση, την υποχρέωση γνωστοποίησης περιστατικών παραβίασης στις εποπτικές αρχές ή στα ίδια τα υποκείμενα.

Η αποτελεσματικότητα των κρυπτογραφικών μέτρων προϋποθέτει, ωστόσο, την ύπαρξη κατάλληλων διαδικασιών διαχείρισης κλειδιών (key management), συμπεριλαμβανομένης της ασφαλούς δημιουργίας, αποθήκευσης, ανανέωσης και ανάκλησής τους. Η ανεπαρκής διαχείριση των κλειδιών δύναται να ακυρώσει στην πράξη τα οφέλη της κρυπτογράφησης και να δημιουργήσει πρόσθετους κινδύνους ασφάλειας.

Συνολικά, η υιοθέτηση ολοκληρωμένης πολιτικής κρυπτογραφίας και η συστηματική εφαρμογή κρυπτογράφησης για δεδομένα αυξημένης κρισιμότητας συνιστούν κρίσιμα μέτρα συμμόρφωσης τόσο με το άρθρο 32 ΓΚΠΔ όσο και με τις απαιτήσεις της NIS2. Τα μέτρα αυτά ενισχύουν την ανθεκτικότητα των βασικών και σημαντικών οντοτήτων, προστατεύουν τα δικαιώματα των φυσικών προσώπων και συμβάλλουν στη δημιουργία ενός αξιόπιστου και ασφαλούς ψηφιακού περιβάλλοντος.

6.2.13 Φυσική και περιβαλλοντική ασφάλεια

Η φυσική ασφάλεια των υποδομών και των χώρων που φιλοξενούν πληροφοριακά συστήματα αποτελεί αναπόσπαστο και ουσιώδες στοιχείο της συνολικής στρατηγικής κυβερνοασφάλειας των βασικών και σημαντικών οντοτήτων. Παρά την αυξανόμενη έμφαση στα ψηφιακά και λογικά μέτρα προστασίας, η φυσική πρόσβαση σε κρίσιμες υποδομές εξακολουθεί να συνιστά σημαντικό παράγοντα κινδύνου, καθώς δύναται να οδηγήσει σε άμεση παραβίαση της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των πληροφοριακών συστημάτων. Στο πλαίσιο αυτό, οι οντότητες οφείλουν να εκπονούν και να εφαρμόζουν γραπτή πολιτική και τεκμηριωμένες διαδικασίες που αφορούν στον φυσικό έλεγχο πρόσβασης (physical access control), καθώς και στην προστασία των εγκαταστάσεων από φυσικούς και περιβαλλοντικούς κινδύνους.

Η πολιτική φυσικής ασφάλειας καθορίζει τις βασικές αρχές, τα επίπεδα προστασίας και τις αρμοδιότητες που σχετίζονται με την πρόσβαση σε χώρους όπου στεγάζονται πληροφοριακά συστήματα, εξοπλισμός ΤΠΕ και κρίσιμες υποδομές. Παράλληλα, λαμβάνει υπόψη κινδύνους όπως πυρκαγιές, πλημμύρες, σεισμοί, διακοπές

ηλεκτροδότησης, ακραία καιρικά φαινόμενα και άλλες περιβαλλοντικές απειλές, οι οποίες δύνανται να επηρεάσουν σοβαρά τη λειτουργία των συστημάτων και την επιχειρησιακή συνέχεια της οντότητας. Η προσέγγιση αυτή ευθυγραμμίζεται με τη φιλοσοφία διαχείρισης κινδύνων της NIS2, η οποία απαιτεί ολοκληρωμένη και πολυεπίπεδη προστασία.

Περαιτέρω, οι βασικές και σημαντικές οντότητες υλοποιούν επαρκή μέτρα φυσικής ασφάλειας και επίβλεψης στην περίμετρο των εγκαταστάσεών τους. Τα μέτρα αυτά περιλαμβάνουν, ενδεικτικά, ελεγχόμενες εισόδους και εξόδους, φυσικά εμπόδια, συστήματα συναγερμού, φωτισμό ασφαλείας, καθώς και συστήματα επιτήρησης, όπως κάμερες κλειστού κυκλώματος (CCTV). Ανάλογα με το επίπεδο επικινδυνότητας και την κρισιμότητα των φιλοξενούμενων υποδομών, η οντότητα δύναται να διαμορφώνει εσωτερικές, διακριτές ζώνες προστασίας, με διαφοροποιημένα επίπεδα ελέγχου πρόσβασης και επιτήρησης, σύμφωνα με την αρχή της αναλογικότητας.

Ιδιαίτερη σημασία αποδίδεται στον περιορισμό της φυσικής πρόσβασης στους χώρους που φιλοξενούν κρίσιμα πληροφοριακά συστήματα. Η πρόσβαση αυτή επιτρέπεται αποκλειστικά σε εξουσιοδοτημένο προσωπικό και πραγματοποιείται με την εφαρμογή κατάλληλων μεθόδων ταυτοποίησης, όπως κάρτες πρόσβασης, βιομετρικά μέσα ή συνδυασμούς αυτών. Παράλληλα, προβλέπεται η συστηματική καταγραφή και παρακολούθηση των εισόδων και εξόδων, μέσω αρχείων καταγραφής (logs) ή συστημάτων εποπτείας, ώστε να διασφαλίζεται η ιχνηλασιμότητα και η λογοδοσία σε περίπτωση περιστατικού ασφάλειας.

Η αποτελεσματικότητα των μέτρων φυσικής ασφάλειας προϋποθέτει τη συνεχή αξιολόγηση και επικαιροποίησή τους, ιδίως όταν μεταβάλλονται οι επιχειρησιακές ανάγκες, οι υποδομές ή το επίπεδο απειλών. Επιπλέον, η εκπαίδευση και η ευαισθητοποίηση του προσωπικού ως προς τις διαδικασίες φυσικής ασφάλειας διαδραματίζουν καθοριστικό ρόλο, καθώς ο ανθρώπινος παράγοντας αποτελεί συχνά κρίσιμο σημείο αποτυχίας ή επιτυχίας των μέτρων προστασίας.

Συνολικά, η θέσπιση και η εφαρμογή ολοκληρωμένων πολιτικών και μέτρων φυσικής και περιβαλλοντικής ασφάλειας ενισχύει ουσιαστικά την ανθεκτικότητα των βασικών και σημαντικών οντοτήτων. Η φυσική προστασία των υποδομών λειτουργεί συμπληρωματικά προς τα τεχνικά και οργανωτικά μέτρα κυβερνοασφάλειας,

συμβάλλοντας στη διασφάλιση της επιχειρησιακής συνέχειας, στη μείωση του κινδύνου σοβαρών περιστατικών και στη συμμόρφωση με τις απαιτήσεις της NIS2 και του εφαρμοστικού εθνικού πλαισίου.

7. ΥΠΟΧΡΕΩΣΕΙΣ ΑΝΑΦΟΡΑΣ ΠΕΡΙΣΤΑΤΙΚΩΝ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ ΚΑΙ ΜΗΧΑΝΙΣΜΟΙ ΕΠΙΧΕΙΡΗΣΙΑΚΗΣ ΣΥΝΕΧΕΙΑΣ ΚΑΤΑ ΤΗ NIS2

7.1 Ανταπόκριση και διαχείριση περιστατικών κυβερνοασφάλειας

Η διαχείριση περιστατικών κυβερνοασφάλειας αποτελεί μία από τις πλέον κρίσιμες και ρητά κατοχυρωμένες υποχρεώσεις των βασικών και σημαντικών οντοτήτων στο πλαίσιο της Οδηγίας (ΕΕ) 2022/2555 (NIS2) και του εφαρμοστικού εθνικού νομοθετικού πλαισίου. Η NIS2 δεν περιορίζεται στη γενική υποχρέωση λήψης προληπτικών μέτρων, αλλά επιβάλλει στις οντότητες την ύπαρξη οργανωμένων, λειτουργικών και δοκιμασμένων μηχανισμών απόκρισης και διαχείρισης περιστατικών κυβερνοασφάλειας, με σκοπό τον περιορισμό των επιπτώσεων και τη διασφάλιση της επιχειρησιακής συνέχειας.

Στο πλαίσιο αυτό, οι βασικές και σημαντικές οντότητες οφείλουν να αναπτύσσουν και να εφαρμόζουν γραπτή πολιτική διαχείρισης περιστατικών κυβερνοασφάλειας, η οποία αποτελεί αναπόσπαστο μέρος του συνολικού συστήματος διαχείρισης κινδύνων. Η πολιτική αυτή καθορίζει σαφώς τους ρόλους και τις αρμοδιότητες του προσωπικού που εμπλέκεται στη διαχείριση περιστατικών, καθώς και τις διαδικασίες εσωτερικής και εξωτερικής αναφοράς προς τις αρμόδιες εθνικές αρχές, σύμφωνα με τα προβλεπόμενα χρονοδιαγράμματα κοινοποίησης της NIS2.

Περαιτέρω, η πολιτική περιλαμβάνει λεπτομερές και τεκμηριωμένο πλάνο για την ανίχνευση, την ανάλυση και την απόκριση σε περιστατικά κυβερνοασφάλειας. Το πλάνο αυτό καλύπτει όλα τα στάδια του κύκλου ζωής ενός περιστατικού, από την αρχική αναγνώριση και αξιολόγηση της σοβαρότητας, έως την εφαρμογή μέτρων περιορισμού, εξάλειψης της απειλής και αποκατάστασης της ορθής λειτουργίας των συστημάτων. Ιδιαίτερη έμφαση αποδίδεται στις διαδικασίες ανάκαμψης και επαναφοράς (recovery), οι οποίες διασφαλίζουν την ταχεία αποκατάσταση κρίσιμων υπηρεσιών και τη μείωση των επιχειρησιακών και οικονομικών επιπτώσεων.

Η NIS2, ωστόσο, δεν αρκείται στη θεωρητική ύπαρξη πολιτικών και διαδικασιών. Αντιθέτως, απαιτεί από τις οντότητες να διασφαλίζουν ότι οι διαδικασίες διαχείρισης περιστατικών είναι πρακτικά εφαρμόσιμες και επαρκώς δοκιμασμένες. Στο πλαίσιο αυτό, οι οντότητες οφείλουν να προβαίνουν σε τακτικές ασκήσεις, δοκιμές και

επαναξιολογήσεις των σχετικών διαδικασιών, προκειμένου να εντοπίζονται αδυναμίες, οργανωτικά κενά ή τεχνικές ελλείψεις και να λαμβάνονται έγκαιρα διορθωτικά μέτρα. Η πρακτική αυτή ενισχύει τη θεσμική ετοιμότητα και την επιχειρησιακή ανθεκτικότητα απέναντι σε πραγματικά περιστατικά.

Παράλληλα, οι βασικές και σημαντικές οντότητες υποχρεούνται να ορίζουν τουλάχιστον έναν υπάλληλο από το προσωπικό τους, ο οποίος αναλαμβάνει τη διαχείριση και τον συντονισμό της διαδικασίας απόκρισης σε περιστατικά κυβερνοασφάλειας. Ο ρόλος αυτός είναι καίριας σημασίας, καθώς διασφαλίζει τη σαφή κατανομή ευθυνών, τη συνεκτική λήψη αποφάσεων και την αποτελεσματική επικοινωνία τόσο εντός της οντότητας όσο και με τις αρμόδιες αρχές.

Σε περιπτώσεις όπου η διαχείριση περιστατικών έχει ανατεθεί σε εξωτερικό ανάδοχο ή πάροχο υπηρεσιών, η NIS2 επιβάλλει τη διατήρηση εσωτερικής εποπτείας. Συγκεκριμένα, η οντότητα οφείλει να ορίζει τουλάχιστον έναν υπάλληλο με ρόλο επίβλεψης της διαδικασίας, διασφαλίζοντας ότι η ευθύνη για τη συμμόρφωση και τη λήψη κρίσιμων αποφάσεων παραμένει σε εσωτερικό επίπεδο και δεν μετακυλίεται αποκλειστικά σε τρίτους.

Συνολικά, η υποχρέωση διαχείρισης περιστατικών κυβερνοασφάλειας, όπως θεσπίζεται από τη NIS2, αναδεικνύει τη μετάβαση από μια παθητική και αποσπασματική προσέγγιση ασφάλειας σε ένα δυναμικό και οργανωμένο μοντέλο επιχειρησιακής ετοιμότητας. Η ύπαρξη τεκμηριωμένων, δοκιμασμένων και εποπτευόμενων διαδικασιών απόκρισης δεν αποτελεί πλέον καλή πρακτική, αλλά νομικά δεσμευτική υποχρέωση, η μη συμμόρφωση με την οποία δύναται να επιφέρει σοβαρές κανονιστικές και διοικητικές συνέπειες για τις βασικές και σημαντικές οντότητες.

7.2 Υποχρέωση κοινοποίησης περιστατικών κυβερνοασφάλειας από βασικές και σημαντικές οντότητες

Η υποχρέωση κοινοποίησης περιστατικών κυβερνοασφάλειας από βασικές και σημαντικές οντότητες συνιστά κεντρικό μηχανισμό του σύγχρονου κανονιστικού πλαισίου για την ενίσχυση της ανθεκτικότητας των ψηφιακών υποδομών και τη διασφάλιση της επιχειρησιακής συνέχειας κρίσιμων και σημαντικών υπηρεσιών.

Στο πλαίσιο αυτό, οι οντότητες υποχρεούνται να κοινοποιούν αμελλητί στην αρμόδια Ομάδα Απόκρισης για Συμβάντα Ασφάλειας Υπολογιστών (CSIRT) της Εθνικής Αρχής Κυβερνοασφάλειας κάθε περιστατικό που έχει ή ενδέχεται να έχει σημαντικό αντίκτυπο στην παροχή των υπηρεσιών τους. Ειδικότερη πρόβλεψη υφίσταται για ορισμένες κατηγορίες οντοτήτων, οι οποίες κοινοποιούν τα περιστατικά στην αρμόδια CSIRT της Εθνικής Υπηρεσίας Πληροφοριών, με ταυτόχρονη ενημέρωση της Εθνικής Αρχής Κυβερνοασφάλειας.

Πέραν της υποχρέωσης κοινοποίησης προς τις αρμόδιες αρχές, οι οικείες οντότητες οφείλουν, χωρίς αδικαιολόγητη καθυστέρηση, να ενημερώνουν και τους αποδέκτες των υπηρεσιών τους, όταν ένα σημαντικό περιστατικό ή μια σημαντική κυβερνοαπειλή ενδέχεται να επηρεάσει αρνητικά την παροχή των εν λόγω υπηρεσιών. Στο πλαίσιο αυτό, οι οντότητες καλούνται όχι μόνο να γνωστοποιούν την ύπαρξη της απειλής ή του περιστατικού, αλλά και να παρέχουν σαφείς πληροφορίες σχετικά με μέτρα ή διορθωτικές ενέργειες που μπορούν να ληφθούν από τους αποδέκτες, συμβάλλοντας έτσι στην πρόληψη ή στον περιορισμό των επιπτώσεων.

Ένα περιστατικό χαρακτηρίζεται ως «σημαντικό» όταν έχει προκαλέσει ή δύναται να προκαλέσει σοβαρή λειτουργική διατάραξη των υπηρεσιών της οντότητας ή σημαντική οικονομική ζημία, καθώς και όταν επιφέρει ή ενδέχεται να επιφέρει ουσιώδη υλική ή μη υλική βλάβη σε νομικά ή φυσικά πρόσωπα. Η αξιολόγηση της σοβαρότητας του περιστατικού αποτελεί κρίσιμο στάδιο, καθώς ενεργοποιεί αυξημένες υποχρεώσεις κοινοποίησης και συνεργασίας με τις αρμόδιες αρχές.

Η διαδικασία κοινοποίησης ακολουθεί κλιμακωτή και χρονικά προσδιορισμένη προσέγγιση. Αρχικά, οι οντότητες υποχρεούνται να υποβάλουν προειδοποίηση χωρίς αδικαιολόγητη καθυστέρηση και, σε κάθε περίπτωση, εντός είκοσι τεσσάρων ωρών από τη στιγμή που αντιλήφθηκαν το σημαντικό περιστατικό. Η προειδοποίηση αυτή περιλαμβάνει, κατά περίπτωση, πληροφορίες σχετικά με το αν το περιστατικό πιθανολογείται ότι προκλήθηκε από παράνομες ή κακόβουλες ενέργειες ή αν ενδέχεται να έχει διασυνοριακό αντίκτυπο. Ακολουθεί, εντός εβδομήντα δύο ωρών, η υποβολή αναλυτικότερης κοινοποίησης περιστατικού, η οποία επικαιροποιεί τα αρχικά στοιχεία και περιλαμβάνει προκαταρκτική αξιολόγηση της σοβαρότητας και των επιπτώσεων, καθώς και τυχόν διαθέσιμες ενδείξεις παραβίασης.

Κατόπιν αιτήματος της Εθνικής Αρχής Κυβερνοασφάλειας, οι οντότητες δύνανται να υποβάλουν ενδιάμεσες εκθέσεις για την εξέλιξη της κατάστασης, ενώ η διαδικασία ολοκληρώνεται με την υποβολή τελικής έκθεσης το αργότερο εντός ενός μηνός από την αρχική κοινοποίηση. Η τελική αυτή έκθεση περιλαμβάνει λεπτομερή περιγραφή του περιστατικού, ανάλυση της φύσης της απειλής ή της βασικής αιτίας, τα μέτρα μετριασμού που έχουν εφαρμοστεί ή βρίσκονται σε εξέλιξη, καθώς και, κατά περίπτωση, τον διασυνοριακό αντίκτυπο. Σε περιπτώσεις όπου το περιστατικό βρίσκεται ακόμη σε εξέλιξη, προβλέπεται η υποβολή έκθεσης προόδου και η κατάθεση τελικής έκθεσης εντός μηνός από την ολοκλήρωση της διαχείρισής του. Ιδιαίτερη ρύθμιση ισχύει για τους παρόχους υπηρεσιών εμπιστοσύνης, οι οποίοι υποχρεούνται να ενημερώνουν την Εθνική Αρχή Κυβερνοασφάλειας εντός είκοσι τεσσάρων ωρών από τη στιγμή που έλαβαν γνώση σημαντικού περιστατικού.

Η Εθνική Αρχή Κυβερνοασφάλειας, από την πλευρά της, υποχρεούται να ανταποκρίνεται αμελλητί στις κοινοποιήσεις, παρέχοντας αρχική αντίδραση και, εφόσον ζητηθεί, καθοδήγηση ή επιχειρησιακές συμβουλές για την εφαρμογή μέτρων μετριασμού. Επιπλέον, δύναται να προσφέρει τεχνική υποστήριξη και, σε περιπτώσεις όπου υπάρχουν ενδείξεις ποινικού χαρακτήρα, να καθοδηγεί την οντότητα ως προς την αναφορά του περιστατικού στις αρμόδιες εισαγγελικές ή αστυνομικές αρχές.

Σε περιπτώσεις διασυνοριακών ή διατομεακών περιστατικών, η συνεργασία επεκτείνεται σε ευρωπαϊκό επίπεδο, με την ενημέρωση των επηρεαζόμενων κρατών μελών και του Οργανισμού της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια. Η ανταλλαγή πληροφοριών πραγματοποιείται με σεβασμό στο ενωσιακό και εθνικό δίκαιο, διασφαλίζοντας την προστασία της ασφάλειας, των εμπορικών συμφερόντων των οντοτήτων και την εμπιστευτικότητα των παρεχόμενων στοιχείων.

Τέλος, προβλέπεται η δυνατότητα ενημέρωσης του κοινού, όταν αυτό κρίνεται αναγκαίο για λόγους πρόληψης ή αντιμετώπισης σημαντικών περιστατικών ή όταν η δημοσιοποίηση εξυπηρετεί το δημόσιο συμφέρον. Παράλληλα, η Εθνική Αρχή Κυβερνοασφάλειας λειτουργεί ως ενιαίο σημείο επαφής, διαβιβάζοντας τις σχετικές κοινοποιήσεις σε άλλα κράτη μέλη και υποβάλλοντας περιοδικές, ανωνυμοποιημένες και συγκεντρωτικές εκθέσεις σε ευρωπαϊκό επίπεδο. Μέσω του πλαισίου αυτού ενισχύεται η διαφάνεια, η συνεργασία και η συλλογική ανθεκτικότητα έναντι των κυβερνοαπειλών,

εδραιώνοντας έναν ολοκληρωμένο μηχανισμό διαχείρισης περιστατικών στον κυβερνοχώρο.

Αμέσως πιο κάτω ακολουθεί φόρμα ενημέρωσής για βασικές και σημαντικές οντότητές κατά NIS2

A	B
Φόρμα Αναφοράς Έγκαιρης Προειδοποίησης 24ωρών για Βασικές και Σημαντικές Οντότητες κατά NIS2	
Η παρούσα φόρμα δύναται να χρησιμοποιηθεί και σε **εθελοντική βάση** από όλους τους φορείς της Ελληνικής επικράτειας, όσον αφορά κυβερνοαπειλές και παρ' ολίγον περιστατικά	
Ημερομηνία αναφοράς Reporting Date	
Τύπος Αναφοράς Report type	
ΕΠΗΡΕΑΖΟΜΕΝΗ ΟΝΤΟΤΗΤΑ **AFFECTED ENTITY**	
Ένταξη στο πεδίο της Οδηγίας NIS2 Within the NIS2 scope	
Βασική ή Σημαντική Οντότητα (NIS2) Essential or Important (NIS2)	
Τομέας κατά NIS2 Sector in NIS2	
Υποτομέας κατά NIS2 Subsector in NIS2	
Επωνυμία της θιγομένης οντότητας Name of affected entity	
Ταχυδρομική Διεύθυνση Address	
Στοιχεία Νόμιμου Εκπροσώπου Legal Representative Information	
Υπεύθυνος Ασφάλειας (ΥΑΣΠΕ/CISO)/Σημείο Επαφής (Ονοματεπώνυμο) Chief Information Security Officer/ Contact Point	
Θέση/ Τίτλος Position / Title	
Τηλέφωνο Telephone Number	
Διεύθυνση Ηλεκτρονικού Ταχυδρομείου E-mail	

ΠΕΡΙΓΡΑΦΗ ΠΕΡΙΣΤΑΤΙΚΟΥ **INCIDENT DESCRIPTION**	
Χρόνος εντοπισμού περιστατικού Date and time of detection of the incident	16/9/2025 και ώρα 2:30 μμ
Εκτιμώμενος χρόνος εκκίνησης περιστατικού Estimated start date of the incident D/M/Y	16/9/2025 και ώρα 2:30 μμ
Βασική αιτία του περιστατικού Indication of the root cause category	☐ Κακόβουλη Ενέργεια ☐ Δυσλειτουργία Συστημάτων ☐ Ανθρώπινο Λάθος ☐ Φυσική Καταστροφή ☐ Άγνωστο
Τύπος περιστατικού Incident type	
Σύντομη Περιγραφή Περιστατικού Incident Description	
Πληροφορίες για το περιστατικό Additional Info	◌ Εν εξελίξει ◉ Ολοκληρωμένα ☐ Επαναλαμβανόμενα
Τεχνικές Λεπτομέρειες* Αναφέρετε Indicators of Compromise (IoCs) σε περίπτωση που έχετε συλλέξει όπως (π.χ. IP addresses, URL addresses, Domains, File hashes, Malware data, Network activity data, E-mail message data, λειτουργικό σύστημα που επηρεάστηκε, υλικό κτλ.)	
Κωδικός αναφοράς περιστατικού θιγόμενης οντότητας Incident reference code provided by the affected entity uniquely identifying reported event	

ΕΚΤΙΜΗΣΗ ΑΝΤΙΚΤΥΠΟΥ IMPACT ESTIMATION	
Παραβίαση Αρχών Ασφάλειας Πληροφοριών Violation of Information Security Principles	☐ Εμπιστευτικότητα ☐ Ακεραιότητα ☐ Διαθεσιμότητα
Τύπος Δεδομένων που τέθηκαν σε κίνδυνο Data types under compromise	☐ Δημόσια ☐ Προσωπικά ☐ Ευαίσθητα ☐ Απόρρητα ☐ Άγνωστο
Τομείς που επηρεάστηκαν Sectors impacted	☐ Ενέργεια ☐ Μεταφορές ☐ Τράπεζες ☐ Υποδομές Χρηματοπιστωτικών Αγορών ☐ Υγεία ☐ Πόσιμο Νερό ☐ Λύματα ☐ Ψηφιακές Υποδομές ☐ Διαχείριση Υπηρεσιών ΤΠΕ ☐ Δημόσια Διοίκηση ☐ Διάστημα ☐ Ταχυδρομικές υπηρεσίες & υπηρεσίες ταχυμεταφορών ☐ Διαχείριση Αποβλήτων ☐ Παραγωγή και διανομή χημικών ☐ Παραγωγή, Επεξεργασία και ☐ Κατασκευαστικός Τομέας ☐ Ψηφιακοί πάροχοι ☐ Έρευνα ☐ Άγνωστο
Βαθμός που επηρεάστηκε η βασική υπηρεσία Information about the extent to which the essential service was	
Βαθμός που επηρεάστηκαν λειτουργικοί τομείς και επιχειρησιακές διαδικασίες Information about the extent to which the operational services were affected	
Διασυνοριακός αντίκτυπος του περιστατικού στις χώρες της Ευρωπαϊκού Οικονομικού Χώρου Cross-border impact of the incident on the countries of the European Economic Area.	○ ΝΑΙ ◉ ΟΧΙ ○ Άγνωστο
Χώρες του Ευρωπαϊκού Οικονομικού Χώρου στις οποίες έχει αντίκτυπο το περιστατικό Affected Member States (European Economic Area)	
Σε περίπτωση υποχρεωτικής αναφοράς αναφερετε συνέπειες ή ενδεχόμενες συνέπειες που καθιστούν το περιστατικό σημαντικό Consequences or potential consequences that make the incident significant	

ΔΙΑΧΕΙΡΙΣΗ ΤΡΕΧΟΥΣΑΣ ΚΑΤΑΣΤΑΣΗΣ CURRENT SITUATION MANAGEMENT	
Ενεργοποίηση Σχεδίου Επιχειρησιακής Συνέχειας (BCP) Activation of BCP (Business Continuity Plan)	○ ΝΑΙ ◉ ΟΧΙ
Ενεργοποίηση Σχεδίου Ανάκαμψης (DRP) Activation of DRP (Disaster Recover Plan)	○ ΝΑΙ ◉ ΟΧΙ
Μέτρα ανάκτησης Recovery measures	
Αναφορά σε άλλες αρχές Reporting to other authorities	☐ Εθνικό CERT ☐ EL-CSIRT (ΕΑΚ) ☐ Διεύθυνση Δίωξης Κυβερνοεγκλήματος ☐ Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ) ☐ Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ) ☐ Τράπεζα της Ελλάδος ☐ Επιτροπή Κεφαλαιαγοράς ☐ Διεύθυνση Κυβερνοάμυνας Υπουργείου Εθνικής Άμυνας (ΓΕΕΘΑ/ ΔΙΚΥΒ) ☐ Αρχή Πολιτικής Αεροπορίας ☐ Άλλο
Ενημέρωση Εμπλεκομένων Stakeholder Notification	☐ Χρήστες που Επηρεάστηκαν ☐ Ενημέρωση Κοινού ☐ Διασυνοριακή Ενημέωση
Ανάγκη υποστήριξης από αρμόδια ομάδα απόκρισης (CSIRT) Support need from the competent CSIRT	○ ΝΑΙ ◉ ΟΧΙ

7.3 Χρονικά στάδια και προθεσμίες κοινοποίησης περιστατικών

Ο ν. 5160/2024, στο άρθρο 16, επιβάλλει χρονικά στάδια κοινοποίησης περιστατικών, στις βασικές και σημαντικές οντότητες, για περιστατικά που έχουν σοβαρό αντίκτυπο, στην παροχή των υπηρεσιών τους. Οι κοινοποιήσεις αυτές πρέπει να γίνονται, στην ομάδα απόκρισης, για συμβάντα που αφορούν, στην ασφάλεια υπολογιστών (CSIRT) της Εθνικής Αρχής Κυβερνοασφάλειας.

Ειδικότερα, οι δημόσιες οντότητες, της Κεντρικής Κυβέρνησης και των Οργανισμών Τοπικής Αυτοδιοίκησης Α΄και Β΄βαθμού, κοινοποιούν τα περιστατικά του

παρόντος άρθρου, στην CSIRT της Εθνικής Υπηρεσίας Πληροφοριών, με ταυτόχρονη ενημέρωση της Εθνικής Αρχής Κυβερνοασφάλειας.

Για την κοινοποίηση των περιστατικών οι οικείες οντότητες υποβάλλουν στην Εθνική Αρχή Κυβερνοασφάλειας:

α) χωρίς αδικαιολόγητη καθυστέρηση και σε κάθε περίπτωση εντός είκοσι τεσσάρων (24) ωρών από τη στιγμή που αντιλήφθηκαν το σημαντικό περιστατικό, προειδοποίηση, η οποία, κατά περίπτωση, αναφέρει αν υπάρχει υποψία ότι το σημαντικό περιστατικό προκλήθηκε από παράνομες ή κακόβουλες ενέργειες ή θα μπορούσε να έχει διασυνοριακό αντίκτυπο,

β) χωρίς αδικαιολόγητη καθυστέρηση και σε κάθε περίπτωση εντός εβδομήντα δύο (72) ωρών από τη στιγμή που αντιλήφθηκαν το σημαντικό περιστατικό, κοινοποίηση περιστατικού, η οποία, κατά περίπτωση, επικαιροποιεί τις πληροφορίες που αναφέρονται στην περ. α) και, επιπλέον, περιλαμβάνει μια αρχική αξιολόγηση του σημαντικού περιστατικού, μεταξύ άλλων της σοβαρότητας και των επιπτώσεών του, καθώς και, εφόσον υπάρχουν, τις ενδείξεις της παραβίασης,

γ) κατόπιν αιτήματος της Εθνικής Αρχής Κυβερνοασφάλειας, ενδιάμεση έκθεση σχετικά με τις σχετικές επικαιροποιήσεις της κατάστασης,

δ) τελική έκθεση το αργότερο εντός ενός (1) μηνός μετά από την υποβολή της αρχικής κοινοποίησης περιστατικού, η οποία περιλαμβάνει τα ακόλουθα:

- ✓ λεπτομερή περιγραφή του περιστατικού, μεταξύ άλλων της σοβαρότητας και των επιπτώσεών του,
- ✓ το είδος της απειλής ή τη βασική αιτία που ενδεχομένως προκάλεσε το περιστατικό,
- ✓ εφαρμοζόμενα και εν εξελίξει μέτρα μετριασμού,
- ✓ κατά περίπτωση, τον διασυνοριακό αντίκτυπο του περιστατικού,
- ✓ σε περίπτωση εν εξελίξει περιστατικού κατά τον χρόνο υποβολής της τελικής έκθεσης, οι οικείες οντότητες υποβάλλουν έκθεση προόδου τη δεδομένη στιγμή και τελική έκθεση εντός ενός (1) μηνός από τον εκ μέρους τους χειρισμό του σημαντικού περιστατικού.

Χρονοδιάγραμμα αναφοράς περιστατικών

7.4 Περιεχόμενο τελικής έκθεσης αναφοράς περιστατικού και οφέλη από την αναφορά περιστατικών

Η τελική έκθεση αναφοράς περιστατικού κυβερνοασφάλειας αποτελεί κρίσιμο στάδιο της διαδικασίας διαχείρισης και κοινοποίησης συμβάντων, καθώς αποτυπώνει με συστηματικό και τεκμηριωμένο τρόπο τη συνολική εικόνα του περιστατικού και των συνεπειών του. Το περιεχόμενό της περιλαμβάνει, κατ' αρχάς, λεπτομερή περιγραφή του περιστατικού, με αναφορά στη φύση του, στη σοβαρότητά του και στις επιχειρησιακές, οικονομικές ή άλλες επιπτώσεις που προκάλεσε ή ενδέχεται να προκαλέσει. Ιδιαίτερη έμφαση δίδεται στον προσδιορισμό του είδους της απειλής ή της βασικής αιτίας που οδήγησε στο περιστατικό, στοιχείο που συμβάλλει ουσιαστικά στην κατανόηση των τρωτών σημείων και στη βελτίωση των μηχανισμών πρόληψης.

Παράλληλα, η τελική έκθεση περιλαμβάνει αναλυτική παρουσίαση των μέτρων μετριασμού που έχουν ήδη εφαρμοστεί, καθώς και εκείνων που βρίσκονται σε εξέλιξη, αποτυπώνοντας τον τρόπο με τον οποίο η οντότητα αντιμετώπισε το περιστατικό και

ενίσχυσε την ανθεκτικότητά της. Κατά περίπτωση, καταγράφεται επίσης ο διασυνοριακός αντίκτυπος του περιστατικού, ιδίως όταν αυτό επηρεάζει ή δύναται να επηρεάσει υπηρεσίες, υποδομές ή χρήστες σε περισσότερα του ενός κράτη. Στις περιπτώσεις όπου το περιστατικό παραμένει σε εξέλιξη κατά τον χρόνο σύνταξης της τελικής έκθεσης, προβλέπεται η υποβολή έκθεσης προόδου, ενώ η οριστική τελική αναφορά κατατίθεται εντός μηνός από την ολοκλήρωση του χειρισμού του περιστατικού.

Η αναφορά περιστατικών κυβερνοασφάλειας δεν συνιστά διακριτική ευχέρεια των οντοτήτων, αλλά δεσμευτική υποχρέωση, με σαφώς καθορισμένα χρονοδιαγράμματα, όπως αυτά προβλέπονται από την Οδηγία NIS2. Όπως χαρακτηριστικά έχει επισημανθεί, η συστηματική και έγκαιρη κοινοποίηση περιστατικών δεν αποσκοπεί αποκλειστικά στη συμμόρφωση με το κανονιστικό πλαίσιο, αλλά λειτουργεί και ως μηχανισμός συλλογικής μάθησης, καθώς η διάχυση πληροφοριών για κυβερνοεπιθέσεις επιτρέπει στους οργανισμούς και στις αρμόδιες αρχές να αντλούν πολύτιμα διδάγματα και να αποφεύγουν την επανάληψη αντίστοιχων λαθών.

Τα οφέλη από την αναφορά περιστατικών είναι πολυεπίπεδα. Σε εθνικό επίπεδο, διασφαλίζεται ότι οι οντότητες επικοινωνούν εγκαίρως με τους αποδέκτες των υπηρεσιών τους που ενδέχεται να επηρεαστούν από σημαντικές κυβερνοαπειλές, παρέχοντάς τους σαφείς οδηγίες, μέτρα ή πρακτικές λύσεις αντιμετώπισης. Σε περιπτώσεις όπου κρίνεται αναγκαίο, οι αποδέκτες ενημερώνονται όχι μόνο για τα μέτρα προστασίας, αλλά και για την ίδια τη φύση της απειλής, ενισχύοντας την επίγνωση κινδύνου και την προληπτική συμπεριφορά.

Επιπλέον, όταν η ευαισθητοποίηση του κοινού κρίνεται αναγκαία είτε για την πρόληψη ενός σημαντικού περιστατικού είτε για την αποτελεσματική αντιμετώπιση ενός εν εξελίξει συμβάντος, ή όταν η γνωστοποίηση εξυπηρετεί το δημόσιο συμφέρον, η Εθνική Αρχή Κυβερνοασφάλειας δύναται, κατόπιν διαβούλευσης με την οικεία οντότητα, να ενημερώσει το κοινό ή να απαιτήσει από την οντότητα τη σχετική ενημέρωση εντός καθορισμένης προθεσμίας. Η διαδικασία αυτή συμβάλλει στη διαφάνεια και στην ενίσχυση της εμπιστοσύνης των πολιτών προς τους οργανισμούς και τις δημόσιες αρχές.

Σε ευρωπαϊκό επίπεδο, και ιδίως σε περιπτώσεις διασυνοριακών περιστατικών, η άμεση ενημέρωση των λοιπών κρατών μελών και των αρμόδιων ευρωπαϊκών φορέων

ενισχύει τον συντονισμό και τη συλλογική ανθεκτικότητα της Ευρωπαϊκής Ένωσης έναντι κυβερνοαπειλών. Η ανταλλαγή πληροφοριών επιτρέπει την έγκαιρη προσαρμογή των μέτρων ασφάλειας και την αποτροπή αλυσιδωτών επιπτώσεων σε διασυνδεδεμένα ψηφιακά οικοσυστήματα.

Συνολικά, οι ανωτέρω ρυθμίσεις και πρακτικές αποτυπώνουν τις κατευθυντήριες γραμμές της Οδηγίας NIS2, οι οποίες, παρότι εφαρμόζονται σε ενωσιακό επίπεδο, επιτρέπουν στα κράτη μέλη να προσαρμόζουν το πλαίσιο αναφοράς περιστατικών στις ιδιαιτερότητες του εθνικού ψηφιακού οικοσυστήματος και στον βαθμό διασύνδεσης των εγχώριων οντοτήτων. Με τον τρόπο αυτό, η αναφορά περιστατικών αναδεικνύεται όχι μόνο ως εργαλείο κανονιστικής συμμόρφωσης, αλλά και ως βασικός πυλώνας πρόληψης, συνεργασίας και συνεχούς βελτίωσης της κυβερνοασφάλειας.

7.5 Επιχειρησιακή συνέχεια και διαχείριση κρίσεων

Η διασφάλιση της επιχειρησιακής συνέχειας και η δυνατότητα ανάκαμψης από καταστροφικά συμβάντα συνιστούν κεντρικό πυλώνα του πλαισίου διαχείρισης κινδύνων κυβερνοασφάλειας που εισάγει η Οδηγία (ΕΕ) 2022/2555 (NIS2). Η Οδηγία αναγνωρίζει ότι η πλήρης πρόληψη κυβερνοπεριστατικών δεν είναι πάντοτε εφικτή και, ως εκ τούτου, επιβάλλει στις βασικές και σημαντικές οντότητες την υποχρέωση να είναι σε θέση να συνεχίζουν ή να αποκαθιστούν εγκαίρως τη λειτουργία των κρίσιμων υπηρεσιών τους μετά από σοβαρά περιστατικά, τεχνικές αστοχίες ή καταστροφικά γεγονότα.

Στο πλαίσιο αυτό, οι βασικές και σημαντικές οντότητες υποχρεούνται να καταρτίζουν και να τηρούν λεπτομερές πλάνο διασφάλισης επιχειρησιακής συνέχειας και ανάκαμψης από καταστροφή (Business Continuity Plan – BCP και Disaster Recovery Plan – DRP). Το πλάνο αυτό βασίζεται στα αποτελέσματα της διαδικασίας αποτίμησης κινδύνων και λαμβάνει υπόψη τόσο τις κυβερνοαπειλές όσο και λοιπούς τεχνικούς, οργανωτικούς και περιβαλλοντικούς κινδύνους που δύνανται να επηρεάσουν τη διαθεσιμότητα των συστημάτων δικτύου και πληροφοριών.

Το πλάνο επιχειρησιακής συνέχειας καθορίζει, κατ' αρχάς, τον σκοπό και το πεδίο εφαρμογής του, προσδιορίζοντας με σαφήνεια ποιες λειτουργίες, υπηρεσίες και

πληροφοριακά συστήματα θεωρούνται κρίσιμα για την αποστολή της οντότητας. Παράλληλα, περιγράφονται αναλυτικά οι ρόλοι και οι αρμοδιότητες του προσωπικού που εμπλέκεται στην ενεργοποίηση και υλοποίηση του πλάνου, διασφαλίζοντας σαφή κατανομή ευθυνών και αποφυγή οργανωτικής σύγχυσης σε συνθήκες κρίσης.

Ιδιαίτερη σημασία αποδίδεται στον καθορισμό σημείων επαφής και καναλιών επικοινωνίας, τόσο σε εσωτερικό επίπεδο όσο και σε επίπεδο επικοινωνίας με εξωτερικούς φορείς, παρόχους υπηρεσιών και αρμόδιες αρχές. Η ύπαρξη προκαθορισμένων μηχανισμών επικοινωνίας συμβάλλει στην έγκαιρη ενημέρωση των εμπλεκόμενων μερών και στη συντονισμένη αντιμετώπιση της κρίσης, περιορίζοντας τον κίνδυνο καθυστερήσεων ή εσφαλμένων αποφάσεων.

Το πλάνο περιλαμβάνει, επίσης, σαφώς προσδιορισμένες συνθήκες ενεργοποίησης, οι οποίες βασίζονται σε αντικειμενικά κριτήρια, όπως η σοβαρότητα ενός περιστατικού, η έκταση της διακοπής υπηρεσιών ή ο αντίκτυπος σε κρίσιμες λειτουργίες. Με τον τρόπο αυτό, αποφεύγεται η αυθαίρετη ή καθυστερημένη ενεργοποίηση των διαδικασιών ανάκαμψης, η οποία θα μπορούσε να επιδεινώσει τις επιπτώσεις του συμβάντος.

Περαιτέρω, το πλάνο καθορίζει τη σειρά των δραστηριοτήτων ανάκαμψης για συγκεκριμένες λειτουργίες και συστήματα, λαμβάνοντας υπόψη την επιχειρησιακή τους προτεραιότητα. Η ιεράρχηση αυτή επιτρέπει την αποδοτικότερη αξιοποίηση των διαθέσιμων πόρων και τη σταδιακή αποκατάσταση των υπηρεσιών με βάση τη σημασία τους για την κοινωνία, την οικονομία και τη λειτουργία της οντότητας.

Τέλος, στο πλαίσιο του πλάνου προσδιορίζονται οι απαιτούμενοι ανθρώπινοι, τεχνικοί και οικονομικοί πόροι για την ορθή και αποτελεσματική υλοποίησή του. Η πρόβλεψη αυτή διασφαλίζει ότι η οντότητα διαθέτει εκ των προτέρων τα μέσα που απαιτούνται για την αντιμετώπιση κρίσιμων καταστάσεων και δεν καλείται να τα εξασφαλίσει εκ των υστέρων, υπό συνθήκες πίεσης.

Η NIS2 δεν αντιμετωπίζει το πλάνο επιχειρησιακής συνέχειας ως στατικό έγγραφο, αλλά ως ζωντανό εργαλείο διαχείρισης κινδύνων. Ως εκ τούτου, οι οντότητες υποχρεούνται να το δοκιμάζουν περιοδικά μέσω ασκήσεων και σεναρίων, καθώς και να το επικαιροποιούν όταν μεταβάλλονται οι λειτουργίες, οι τεχνολογίες ή το περιβάλλον

απειλών. Με τον τρόπο αυτό, η επιχειρησιακή συνέχεια αναδεικνύεται σε βασικό στοιχείο ανθεκτικότητας και κανονιστικής συμμόρφωσης στο σύγχρονο ψηφιακό περιβάλλον.

8 ΑΣΦΑΛΕΙΑ ΕΦΟΔΙΑΣΤΙΚΗΣ ΑΛΥΣΙΔΑΣ ΚΑΙ ΔΙΑΧΕΙΡΙΣΗ ΚΙΝΔΥΝΩΝ ΤΡΙΤΩΝ ΜΕΡΩΝ ΣΤΟ ΠΛΑΙΣΙΟ ΤΗΣ NIS 2 ΚΑΙ ΤΟΥ Ν. 5160/2024: ΚΑΝΟΝΙΣΤΙΚΗ ΘΕΜΕΛΙΩΣΗ ΚΑΙ ΜΕΘΟΔΟΛΟΓΙΚΟ ΠΛΑΙΣΙΟ ΣΥΜΜΟΡΦΩΣΗΣ

8.1 Πολιτική διαχείρισης και ταξινόμηση κρισιμότητας προμηθευτών Τ.Π.Ε. στο πλαίσιο της ασφάλειας εφοδιαστικής αλυσίδας

Η διαχείριση της ασφάλειας της εφοδιαστικής αλυσίδας Τεχνολογιών Πληροφορικής και Επικοινωνιών (Τ.Π.Ε.) αποτελεί κρίσιμη διάσταση της συνολικής στρατηγικής κυβερνοασφάλειας των βασικών και σημαντικών οντοτήτων, ιδίως λόγω της αυξανόμενης εξάρτησής τους από εξωτερικούς προμηθευτές και παρόχους ψηφιακών υπηρεσιών. Στο πλαίσιο αυτό, οι οντότητες οφείλουν να εκπονούν και να εφαρμόζουν σαφή πολιτική και διαδικασίες που διέπουν τις σχέσεις τους με προμηθευτές και παρόχους υπηρεσιών Τ.Π.Ε., με σκοπό τον συστηματικό εντοπισμό, την αξιολόγηση και τη διαχείριση των κινδύνων που απορρέουν από τη χρήση προϊόντων και υπηρεσιών τρίτων.

Κεντρικό στοιχείο της πολιτικής αυτής αποτελεί η κατάρτιση και η διαρκής επικαιροποίηση καταλόγου των άμεσων προμηθευτών και παρόχων υπηρεσιών Τ.Π.Ε. της οντότητας. Ο κατάλογος περιλαμβάνει, ενδεικτικά, παραγωγούς και κατασκευαστές υλικού και λογισμικού, παρόχους υπηρεσιών νεφοϋπολογιστικής, παρόχους διαχειριζόμενων υπηρεσιών, καθώς και παρόχους διαχειριζόμενων υπηρεσιών ασφάλειας. Για κάθε προμηθευτή καταγράφονται κατ' ελάχιστον τα βασικά σημεία επαφής, καθώς και τα συγκεκριμένα προϊόντα και υπηρεσίες Τ.Π.Ε. που παρέχονται προς την οντότητα, διασφαλίζοντας σαφή εικόνα των εξαρτήσεων και των διασυνδέσεων.

Περαιτέρω, ο κατάλογος αυτός συνοδεύεται από διαδικασία ταξινόμησης των προμηθευτών και παρόχων υπηρεσιών Τ.Π.Ε. σε επίπεδα κρισιμότητας, με βάση παράγοντες όπως η σημασία των παρεχόμενων υπηρεσιών για την επιχειρησιακή συνέχεια, η πρόσβαση σε κρίσιμα συστήματα ή δεδομένα και ο δυνητικός αντίκτυπος μιας διακοπής ή παραβίασης ασφάλειας. Η ταξινόμηση αυτή επιτρέπει την αναλογική εφαρμογή μέτρων ελέγχου και εποπτείας, καθώς και τη στοχευμένη ενίσχυση των απαιτήσεων ασφάλειας για τους προμηθευτές υψηλής κρισιμότητας.

Συνολικά, η θεσμοθέτηση πολιτικών και διαδικασιών για τη διαχείριση των κινδύνων της εφοδιαστικής αλυσίδας Τ.Π.Ε. συμβάλλει καθοριστικά στην ενίσχυση της ανθεκτικότητας των βασικών και σημαντικών οντοτήτων, περιορίζοντας την έκθεσή τους σε έμμεσες απειλές κυβερνοασφάλειας και ενισχύοντας τη διαφάνεια, τη λογοδοσία και την επιχειρησιακή συνέχεια σε ένα ολοένα και πιο διασυνδεδεμένο ψηφιακό περιβάλλον.

8.2 Η εξελικτική δυναμική των επιθέσεων εφοδιαστικής αλυσίδας σύμφωνα με τον ENISA

Η ανάλυση των επιθέσεων στην εφοδιαστική αλυσίδα (supply chain attacks) έχει αναδειχθεί σε κεντρικό άξονα της ευρωπαϊκής πολιτικής κυβερνοασφάλειας. Σύμφωνα με τον European Union Agency for Cybersecurity, οι επιθέσεις αυτού του τύπου δεν αποτελούν πλέον μεμονωμένα περιστατικά υψηλής πολυπλοκότητας, αλλά διαμορφώνουν μια σταθερή και αυξανόμενη απειλητική τάση με έντονο συστημικό χαρακτήρα. Στις εκθέσεις ENISA Threat Landscape for Supply Chain Attacks, η Υπηρεσία επισημαίνει ότι οι επιτιθέμενοι στοχεύουν όλο και περισσότερο σε παρόχους λογισμικού, διαχειριζόμενες υπηρεσίες (MSPs), παρόχους υπηρεσιών νεφοϋπολογιστικής και προμηθευτές κρίσιμων ψηφιακών υποδομών, με σκοπό την έμμεση πρόσβαση σε μεγάλο αριθμό θυμάτων.

Σύμφωνα με τον ENISA, η ουσία των επιθέσεων στην εφοδιαστική αλυσίδα έγκειται στη στρατηγική εκμετάλλευση της εμπιστοσύνης μεταξύ οργανισμών και των προμηθευτών τους. Οι οργανισμοί βασίζονται σε προϊόντα, ενημερώσεις λογισμικού, βιβλιοθήκες κώδικα και υπηρεσίες τρίτων για τη λειτουργία των συστημάτων τους. Όταν

ένας επιτιθέμενος καταφέρει να παραβιάσει έναν προμηθευτή, αποκτά τη δυνατότητα να διεισδύσει σε πολλαπλούς οργανισμούς χωρίς να χρειάζεται να τους στοχεύσει άμεσα. Πρόκειται για επιθέσεις με «πολλαπλασιαστικό αποτέλεσμα», καθώς μία επιτυχής παραβίαση σε έναν προμηθευτή ανώτερου επιπέδου της εφοδιαστικής αλυσίδας (upstream supplier) μπορεί να προκαλέσει επιπτώσεις σε οργανισμούς κατώτερου επιπέδου της αλυσίδας (downstream entities), επηρεάζοντας εκατοντάδες ή ακόμη και χιλιάδες οργανισμούς.

Ο ENISA καταγράφει αύξηση τόσο στον αριθμό όσο και στην πολυπλοκότητα των επιθέσεων αυτών. Οι επιθέσεις αφορούν κυρίως:

(α) συμβιβασμό μηχανισμών ενημέρωσης λογισμικού,

(β) εισαγωγή κακόβουλου κώδικα σε νόμιμες βιβλιοθήκες,

(γ) εκμετάλλευση ευπαθειών σε ευρέως διαδεδομένα λογισμικά στοιχεία (widely- used components), και

(δ) κατάχρηση νόμιμων διαπιστευτηρίων διαχειριστών υπηρεσιών. Ιδιαίτερη έμφαση δίδεται στις επιθέσεις που αξιοποιούν ανοιχτό κώδικα (open source), καθώς μεγάλος αριθμός οργανισμών εξαρτάται από κοινές βιβλιοθήκες χωρίς πλήρη ορατότητα ως προς την ακεραιότητά τους.

Ένα κρίσιμο εύρημα του ENISA αφορά τη μετατόπιση της απειλής από παραδοσιακούς κρατικούς δρώντες προς ένα ευρύτερο φάσμα επιτιθέμενων, συμπεριλαμβανομένων οργανωμένων εγκληματικών ομάδων που αξιοποιούν τεχνικές επιθέσεων στην εφοδιαστική αλυσίδα (supply chain techniques) για την πραγματοποίηση εκστρατειών ransomware (ransomware campaigns). Υπό τις συνθήκες αυτές, η εφοδιαστική αλυσίδα μετατρέπεται σε εργαλείο οικονομικής εκμετάλλευσης, καθώς η παραβίαση ενός παρόχου υπηρεσιών πληροφορικής μπορεί να οδηγήσει σε ταυτόχρονες επιθέσεις εναντίον πολλαπλών πελατών του.

Σύμφωνα με τον ENISA, βασικό χαρακτηριστικό των επιθέσεων αυτών είναι η δυσκολία εντοπισμού τους. Η κακόβουλη δραστηριότητα συχνά ενσωματώνεται σε νόμιμες διαδικασίες (π.χ. ενημέρωση λογισμικού), γεγονός που καθιστά την ανίχνευση περίπλοκη. Επιπλέον, η αλυσίδα ευθύνης είναι πολυεπίπεδη: ο τελικός οργανισμός μπορεί να μην έχει άμεση συμβατική σχέση με τον ανωτέρου επιπέδου στην εφοδιαστική

αλυσίδα προμηθευτή όπου εντοπίζεται η αρχική παραβίαση. Αυτό δημιουργεί προκλήσεις τόσο τεχνικής απόκρισης όσο και νομικής λογοδοσίας.

Ο ENISA επισημαίνει επίσης την έννοια του κινδύνου συγκέντρωσης (concentration risk). Η εξάρτηση μεγάλου αριθμού οργανισμών από περιορισμένο αριθμό υπερκλιμακούμενων παρόχων υπολογιστικού νέφους (hyperscale cloud providers) ή από συγκεκριμένους κατασκευαστές λογισμικού δημιουργεί συστημικό κίνδυνο για τα ψηφιακά οικοσυστήματα. Υπό τις συνθήκες αυτές, μια επιτυχής επίθεση σε τέτοιους κομβικούς παρόχους μπορεί να έχει διατομεακές συνέπειες, επηρεάζοντας κρίσιμους τομείς όπως η ενέργεια, η υγεία, οι μεταφορές και οι χρηματοοικονομικές υπηρεσίες.

Σε επίπεδο επιπτώσεων, ο ENISA καταγράφει ότι οι συνέπειες των επιθέσεων στην εφοδιαστική αλυσίδα (supply chain attacks) υπερβαίνουν την απλή παραβίαση δεδομένων. Οι επιθέσεις αυτές μπορούν να οδηγήσουν σε διακοπή υπηρεσιών, απώλεια επιχειρησιακής συνέχειας, σημαντική φθορά της φήμης των οργανισμών, επιβολή νομικών κυρώσεων και οικονομικές απώλειες μεγάλης κλίμακας. Ιδίως για οργανισμούς που εμπίπτουν στο πεδίο εφαρμογής της Οδηγίας (ΕΕ) 2022/2555 (Directive (EU) 2022/2555 – NIS2), οι επιθέσεις αυτές συνδέονται άμεσα με τις υποχρεώσεις διαχείρισης κινδύνου και τη λογοδοσία της διοίκησης. Στο πλαίσιο αυτό, η ασφάλεια της εφοδιαστικής αλυσίδας αναδεικνύεται σε κρίσιμο στοιχείο της συνολικής στρατηγικής κυβερνοασφάλειας των οργανισμών που υπάγονται στο κανονιστικό πεδίο της οδηγίας.

Απέναντι σε αυτή την απειλητική τοπογραφία, ο ENISA προτείνει μια πολυεπίπεδη προσέγγιση με έμφαση στη διαφάνεια, την ιχνηλασιμότητα και την συνεχή παρακολούθηση. Κεντρικά εργαλεία της στρατηγικής αυτής αποτελούν η χαρτογράφηση της εφοδιαστικής αλυσίδας, η κατάρτιση καταλόγων προμηθευτών, η αξιολόγηση επιπέδου κρισιμότητας έκαστου προμηθευτή, καθώς και η ενσωμάτωση ρητρών ασφάλειας σε συμβάσεις. Παράλληλα, προωθείται η χρήση Software Bill of Materials (SBOM), ώστε οι οργανισμοί να γνωρίζουν ποια επιμέρους στοιχεία περιλαμβάνονται στα συστήματά τους.

Ιδιαίτερη σημασία αποδίδεται στη συνεχή παρακολούθηση (continuous monitoring) και στη συνεργασία μεταξύ δημόσιου και ιδιωτικού τομέα. Η ανταλλαγή πληροφοριών για ευπάθειες και απειλές, μέσω εθνικών και ευρωπαϊκών μηχανισμών, θεωρείται

κρίσιμη για τον έγκαιρο εντοπισμό επιθέσεων που διαχέονται διαμέσου της εφοδιαστικής αλυσίδας.

Συνολικά, σύμφωνα με τον ENISA, οι επιθέσεις εφοδιαστικής αλυσίδας συνιστούν μία από τις πλέον σοβαρές και σύνθετες μορφές κυβερνοαπειλής της τελευταίας δεκαετίας. Δεν πρόκειται απλώς για τεχνικό πρόβλημα ασφάλειας, αλλά για ζήτημα συστημικής ανθεκτικότητας. Η αντιμετώπισή τους απαιτεί συνδυασμό τεχνικών μέτρων, οργανωτικών πολιτικών, νομικών εργαλείων και διακρατικής συνεργασίας. Η κατανόηση της απειλητικής τοπογραφίας που σκιαγραφεί ο ENISA αποτελεί αναγκαία προϋπόθεση για τη διαμόρφωση αποτελεσματικών στρατηγικών διαχείρισης κινδύνων και για την ενίσχυση της ασφάλειας της ευρωπαϊκής ψηφιακής εφοδιαστικής αλυσίδας.

8.3 Κανονιστικές υποχρεώσεις με βάση το άρθρο 21 της NIS 2 για την ασφάλεια εφοδιαστικής αλυσίδας

Το άρθρο 21 της Οδηγίας NIS2 συνιστά τον πυρήνα του κανονιστικού πλαισίου διαχείρισης κινδύνων που θεσπίζει η Οδηγία, εισάγοντας σαφείς και δεσμευτικές υποχρεώσεις για τις βασικές και σημαντικές οντότητες. Η διάταξη αυτή μετατοπίζει το κέντρο βάρους από μια αποσπασματική, τεχνικού χαρακτήρα αντίληψη της κυβερνοασφάλειας σε ένα ολιστικό σύστημα διακυβέρνησης κινδύνων, το οποίο περιλαμβάνει όχι μόνο την εσωτερική οργανωτική δομή της οντότητας, αλλά και το σύνολο των εξωτερικών της εξαρτήσεων.

Κεντρικό στοιχείο του άρθρου 21 αποτελεί η υποχρέωση υιοθέτησης «κατάλληλων και αναλογικών τεχνικών και οργανωτικών μέτρων» για τη διαχείριση των κινδύνων που απειλούν την ασφάλεια των δικτύων και των συστημάτων πληροφοριών. Η έννοια της αναλογικότητας δεν είναι τυπική, αλλά ουσιαστική: τα μέτρα πρέπει να λαμβάνουν υπόψη το μέγεθος της οντότητας, τον βαθμό έκθεσής της σε κινδύνους, την πιθανότητα και τη σοβαρότητα των επιπτώσεων, καθώς και τη σημασία της για την κοινωνία και την οικονομία. Η αξιολόγηση αυτή αποκτά ιδιαίτερη σημασία όταν οι κίνδυνοι δεν προέρχονται άμεσα από την ίδια την οντότητα, αλλά από την εφοδιαστική της αλυσίδα.

Η NIS 2 εισάγει ρητή αναφορά στην ασφάλεια της εφοδιαστικής αλυσίδας, αναγνωρίζοντας ότι οι σύγχρονες ψηφιακές υποδομές λειτουργούν εντός ενός

πλέγματος αλληλεξαρτήσεων. Οι βασικές και σημαντικές οντότητες εξαρτώνται σε μεγάλο βαθμό από παρόχους λογισμικού, κατασκευαστές υλικού, παρόχους υπηρεσιών νεφοϋπολογιστικής, διαχειριζόμενες υπηρεσίες (managed services) και παρόχους υπηρεσιών ασφάλειας. Η παραβίαση ή αστοχία ενός εκ των κρίκων αυτής της αλυσίδας μπορεί να επιφέρει εκτεταμένες και πολλαπλασιαστικές συνέπειες.

Στο πλαίσιο αυτό, το άρθρο 21 επιβάλλει την ενσωμάτωση της **διαχείρισης κινδύνων τρίτων μερών** (Third Party Risk Management – TPRM) στον πυρήνα του συστήματος κυβερνοασφάλειας της οντότητας. Δεν αρκεί η απλή επιλογή αξιόπιστων προμηθευτών, αλλά· απαιτείται συστηματική και τεκμηριωμένη αξιολόγηση των κινδύνων που απορρέουν από τα προϊόντα και τις υπηρεσίες που αυτοί παρέχουν. Η αξιολόγηση αυτή περιλαμβάνει, μεταξύ άλλων, τον έλεγχο των πρακτικών ασφάλειας των προμηθευτών, τη συμμόρφωσή τους με διεθνή πρότυπα, την διαχείριση ευπαθειών, καθώς και την ικανότητά τους να ανταποκριθούν σε περιστατικά ασφάλειας.

Ιδιαίτερη μνεία γίνεται στους άμεσους προμηθευτές (direct suppliers) και στους παρόχους υπηρεσιών (service providers), ιδίως όταν αυτοί διαθέτουν πρόσβαση σε κρίσιμα συστήματα ή επεξεργάζονται ευαίσθητα δεδομένα. Η πρόσβαση αυτή δημιουργεί έναν δίαυλο δυνητικής εισόδου απειλών, είτε μέσω κακόβουλων ενεργειών είτε μέσω αδυναμιών ασφαλείας. Κατά συνέπεια, οι οντότητες οφείλουν να εφαρμόζουν ενισχυμένα μέτρα εποπτείας και ελέγχου για τους προμηθευτές υψηλής κρισιμότητας, περιλαμβανομένων συμβατικών ρητρών ασφάλειας, δικαιωμάτων ελέγχου (audit rights), υποχρεώσεων γνωστοποίησης περιστατικών και απαιτήσεων συμμόρφωσης με συγκεκριμένα πρότυπα.

Το άρθρο 21 προβλέπει επίσης την υιοθέτηση διαδικασιών διαχείρισης περιστατικών και επιχειρησιακής συνέχειας που λαμβάνουν υπόψη τις εξαρτήσεις από τρίτους. Η ανθεκτικότητα μιας οντότητας δεν μπορεί να αξιολογηθεί αποκομμένα από την ανθεκτικότητα των προμηθευτών της. Ως εκ τούτου, η αξιολόγηση κινδύνων οφείλει να περιλαμβάνει σενάρια διακοπής υπηρεσιών, παραβίασης δεδομένων ή αποτυχίας κρίσιμων προμηθευτών, καθώς και σχέδια εναλλακτικής παροχής (fallback arrangements).

Επιπλέον, η διάταξη συνδέεται με την υποχρέωση εποπτείας και λογοδοσίας της διοίκησης. Τα διοικητικά όργανα των οντοτήτων φέρουν ευθύνη για την έγκριση και την

παρακολούθηση των μέτρων διαχείρισης κινδύνων, συμπεριλαμβανομένων εκείνων που αφορούν την εφοδιαστική αλυσίδα. Η ευθύνη αυτή αναδεικνύει τη διαχείριση κινδύνων τρίτων μερών ως ζήτημα εταιρικής διακυβέρνησης και όχι απλώς τεχνικής συμμόρφωσης.

Η πρακτική εφαρμογή του άρθρου 21 προϋποθέτει την δημιουργία καταλόγου προμηθευτών, την ταξινόμησή τους σε επίπεδα κρισιμότητας και την αναλογική επιβολή μέτρων. Οι οντότητες οφείλουν να τεκμηριώνουν τις αξιολογήσεις τους και να διατηρούν αποδεικτικά στοιχεία συμμόρφωσης, ώστε να είναι σε θέση να ανταποκριθούν σε ελέγχους των αρμόδιων εποπτικών αρχών.

Συνολικά, το άρθρο 21 της NIS 2 μετασχηματίζει την έννοια της κυβερνοασφάλειας σε ένα πολυεπίπεδο σύστημα διαχείρισης κινδύνων, στο οποίο η εφοδιαστική αλυσίδα καταλαμβάνει κεντρική θέση. Η κανονιστική αυτή εξέλιξη αναγνωρίζει ότι η ασφάλεια ενός οργανισμού είναι άρρηκτα συνδεδεμένη με την ασφάλεια των συνεργατών και των προμηθευτών του, επιβάλλοντας μια προσέγγιση που συνδυάζει τεχνικά μέτρα, οργανωτικές διαδικασίες, συμβατικές δεσμεύσεις και διοικητική εποπτεία. Μέσω της ενσωμάτωσης της διαχείρισης κινδύνων τρίτων μερών στο κανονιστικό πλαίσιο, η NIS 2 επιδιώκει την ενίσχυση της συνολικής ανθεκτικότητας των κρίσιμων και σημαντικών οντοτήτων εντός της Ευρωπαϊκής Ένωσης.

8.4 Υποχρεώσεις κατά τον Ν. 5160/2024 αναφορικά με την ασφάλεια της εφοδιαστικής αλυσίδας

Ο Νόμος 5160/2024, με τον οποίο ενσωματώθηκε στην ελληνική έννομη τάξη η Directive (EU) 2022/2555 (NIS 2), θεσπίζει ένα δεσμευτικό και συστηματοποιημένο πλαίσιο υποχρεώσεων αναφορικά με τη διαχείριση κινδύνων που απορρέουν από την εφοδιαστική αλυσίδα Τεχνολογιών Πληροφορικής και Επικοινωνιών. Η ασφάλεια των σχέσεων με προμηθευτές και παρόχους υπηρεσιών Τ.Π.Ε. δεν αντιμετωπίζεται πλέον ως συμπληρωματική διάσταση της κυβερνοασφάλειας, αλλά ως αναπόσπαστο στοιχείο της συνολικής στρατηγικής διαχείρισης κινδύνων των βασικών και σημαντικών οντοτήτων.

Στο πλαίσιο της ενσωμάτωσης της Οδηγίας στο εθνικό δίκαιο, ο Ν. 5160/2024 μετατρέπει τις γενικές κανονιστικές κατευθύνσεις της NIS 2 σε συγκεκριμένες και ελέγξιμες υποχρεώσεις. Οι οντότητες που εμπίπτουν στο πεδίο εφαρμογής του νόμου

υποχρεούνται να θεσπίζουν, να εφαρμόζουν και να τεκμηριώνουν πολιτικές και διαδικασίες διαχείρισης κινδύνων που καλύπτουν ρητώς και τους κινδύνους που προκύπτουν από τρίτα μέρη. Η υποχρέωση αυτή περιλαμβάνει τη συστηματική χαρτογράφηση των άμεσων προμηθευτών και παρόχων υπηρεσιών Τ.Π.Ε., την αξιολόγηση της κρισιμότητας των παρεχόμενων προϊόντων και υπηρεσιών, καθώς και την εκτίμηση του δυνητικού αντίκτυπου που θα είχε μια διακοπή λειτουργίας ή ένα περιστατικό ασφάλειας σε επίπεδο προμηθευτή.

Η διαχείριση της ασφάλειας της εφοδιαστικής αλυσίδας, κατά τον νόμο, δεν περιορίζεται στην αρχική επιλογή ενός προμηθευτή. Αντιθέτως, προϋποθέτει συνεχή εποπτεία και επαναξιολόγηση, ιδίως όταν πρόκειται για προμηθευτές υψηλής κρισιμότητας, οι οποίοι έχουν πρόσβαση σε κρίσιμα πληροφοριακά συστήματα ή επεξεργάζονται ευαίσθητα δεδομένα. Οι οργανισμοί οφείλουν να διασφαλίζουν ότι οι συμβάσεις τους με προμηθευτές ενσωματώνουν ρήτρες ασφάλειας, υποχρεώσεις γνωστοποίησης περιστατικών, δικαιώματα ελέγχου και απαιτήσεις συμμόρφωσης με αναγνωρισμένα πρότυπα κυβερνοασφάλειας. Με τον τρόπο αυτό, η διαχείριση κινδύνων αποκτά σαφή νομική διάσταση και ενισχύεται η δυνατότητα παρέμβασης της οντότητας σε περίπτωση αδυναμίας ή πλημμελούς συμμόρφωσης του συνεργάτη της.

Καθοριστικό ρόλο στην εφαρμογή του πλαισίου διαδραματίζουν οι αρμόδιες εποπτικές αρχές, οι οποίες ορίζονται από τον Ν. 5160/2024. Οι αρχές αυτές διαθέτουν εκτεταμένες αρμοδιότητες ελέγχου, τόσο προληπτικού όσο και κατασταλτικού χαρακτήρα. Σε προληπτικό επίπεδο, δύνανται να ζητούν από τις οντότητες την υποβολή πολιτικών διαχείρισης κινδύνων τρίτων μερών, καταλόγων προμηθευτών και τεκμηρίωσης αξιολόγησης κρισιμότητας. Η υποχρέωση τεκμηρίωσης καθίσταται ιδιαίτερα σημαντική, καθώς οι οργανισμοί οφείλουν να αποδεικνύουν ότι έχουν λάβει αναλογικά και κατάλληλα μέτρα σε σχέση με το προφίλ κινδύνου τους.

Σε κατασταλτικό επίπεδο, οι εποπτικές αρχές μπορούν να διενεργούν επιθεωρήσεις, να απαιτούν πρόσβαση σε πληροφορίες και έγγραφα, καθώς και να αξιολογούν την αποτελεσματικότητα των μέτρων που εφαρμόζονται. Ιδίως σε περιπτώσεις περιστατικών κυβερνοασφάλειας που σχετίζονται με προμηθευτές, εξετάζεται εάν η οντότητα είχε προηγουμένως εντοπίσει τον σχετικό κίνδυνο, εάν είχε ενσωματώσει κατάλληλες συμβατικές ρήτρες και εάν είχε προβλέψει εναλλακτικές

διαδικασίες διασφάλισης της επιχειρησιακής συνέχειας. Η εποπτεία, επομένως, δεν περιορίζεται σε τυπικό έλεγχο ύπαρξης πολιτικών, αλλά επεκτείνεται στην αξιολόγηση της ουσιαστικής τους αποτελεσματικότητας.

Το καθεστώς κυρώσεων που προβλέπει ο Ν. 5160/2024 ενισχύει περαιτέρω τον δεσμευτικό χαρακτήρα των υποχρεώσεων ασφάλειας εφοδιαστικής αλυσίδας. Σε περίπτωση μη συμμόρφωσης, οι εποπτικές αρχές μπορούν να επιβάλουν διοικητικά πρόστιμα, τα οποία καθορίζονται με βάση την αρχή της αναλογικότητας, λαμβάνοντας υπόψη τη σοβαρότητα και τη διάρκεια της παράβασης, τον βαθμό υπαιτιότητας, καθώς και τον αντίκτυπο στη λειτουργία βασικών υπηρεσιών. Πέραν των χρηματικών κυρώσεων, είναι δυνατή η επιβολή διορθωτικών μέτρων με συγκεκριμένη προθεσμία συμμόρφωσης, καθώς και άλλων περιοριστικών παρεμβάσεων, ιδίως όταν διαπιστώνεται σοβαρός και άμεσος κίνδυνος για τη δημόσια ασφάλεια ή τη συνέχεια κρίσιμων λειτουργιών.

Ιδιαίτερη σημασία έχει και η ευθύνη των διοικητικών οργάνων των οντοτήτων, τα οποία υποχρεούνται να εγκρίνουν και να παρακολουθούν την εφαρμογή των μέτρων διαχείρισης κινδύνων. Η διάσταση αυτή εντάσσει την ασφάλεια της εφοδιαστικής αλυσίδας στο πεδίο της εταιρικής διακυβέρνησης, καθιστώντας τη συμμόρφωση όχι μόνο τεχνικό, αλλά και διοικητικό ζήτημα.

Συνολικά, ο Ν. 5160/2024 διαμορφώνει ένα συνεκτικό εθνικό πλαίσιο για την ασφάλεια της εφοδιαστικής αλυσίδας, το οποίο συνδυάζει κανονιστικές υποχρεώσεις, εποπτική παρακολούθηση και αποτελεσματικό σύστημα κυρώσεων. Η ενσωμάτωση των απαιτήσεων της NIS 2 στο ελληνικό δίκαιο ενισχύει τη θεσμική θωράκιση των βασικών και σημαντικών οντοτήτων έναντι συστημικών κινδύνων που ανακύπτουν από τις ψηφιακές τους εξαρτήσεις, συμβάλλοντας στη συνολική ανθεκτικότητα του εθνικού οικοσυστήματος κυβερνοασφάλειας.

8.5 Καλές πρακτικές ασφάλειας εφοδιαστικής αλυσίδας σύμφωνα με τον ENISA

Σύμφωνα με τον European Union Agency for Cybersecurity, η ασφάλεια της εφοδιαστικής αλυσίδας Τεχνολογιών Πληροφορικής και Επιχειρησιακής Τεχνολογίας (ICT/OT) αποτελεί θεμελιώδη παράγοντα για τη συνολική ανθεκτικότητα των

οργανισμών που παρέχουν κρίσιμες και σημαντικές υπηρεσίες. Σύμφωνα με το κατευθυντήριο κείμενο Good Practices for Supply Chain Cybersecurity (Ιούνιος 2023), ο ENISA διαμορφώνει ένα συνεκτικό πλαίσιο καλών πρακτικών που αποσκοπεί στην ενίσχυση της διακυβέρνησης, της διαχείρισης κινδύνων και της επιχειρησιακής ωριμότητας των οργανισμών ως προς τις εξαρτήσεις τους από προμηθευτές και παρόχους υπηρεσιών.

Πρώτη και κεντρική καλή πρακτική αποτελεί η υιοθέτηση στρατηγικής εταιρικής προσέγγισης. Η ασφάλεια της εφοδιαστικής αλυσίδας δεν πρέπει να αντιμετωπίζεται αποσπασματικά ή αποκλειστικά ως τεχνικό ζήτημα, αλλά να εντάσσεται σε μια συνολική στρατηγική κυβερνοασφάλειας, εγκεκριμένη από τη διοίκηση και υποστηριζόμενη από επαρκείς πόρους. Ο ENISA επισημαίνει ότι απαιτείται σαφής κατανομή ρόλων και αρμοδιοτήτων, καθώς και η σύσταση διατμηματικών ομάδων που να περιλαμβάνουν στελέχη από τομείς όπως η ασφάλεια πληροφοριών, οι προμήθειες, το νομικό τμήμα και η διαχείριση κινδύνων. Η ενεργή συμμετοχή της διοίκησης διασφαλίζει ότι οι αποφάσεις σχετικά με προμηθευτές και τεχνολογικές εξαρτήσεις λαμβάνονται με γνώμονα το συνολικό προφίλ κινδύνου του οργανισμού.

Δεύτερη βασική πρακτική είναι η υιοθέτηση προσέγγισης βασισμένης στον κίνδυνο (risk-based approach) για τη διαχείριση της εφοδιαστικής αλυσίδας. Οι οργανισμοί οφείλουν να χαρτογραφούν τους άμεσους προμηθευτές και παρόχους υπηρεσιών τους, να προσδιορίζουν τα κρίσιμα προϊόντα και υπηρεσίες, και να αξιολογούν τον πιθανό αντίκτυπο μιας διακοπής ή παραβίασης. Ιδιαίτερη σημασία αποδίδεται στον εντοπισμό κρίσιμων εξαρτήσεων και «μοναδικών σημείων αποτυχίας» (single points of failure), καθώς και στη χαρτογράφηση λογισμικών εξαρτήσεων έως το επίπεδο βιβλιοθηκών και επιμέρους στοιχείων. Ο ENISA υπογραμμίζει ότι η αξιολόγηση κινδύνου δεν πρέπει να είναι εφάπαξ διαδικασία, αλλά να συνοδεύεται από συνεχή παρακολούθηση μεταβολών στο προφίλ κινδύνου των προμηθευτών, λαμβάνοντας υπόψη νέες απειλές, γεωπολιτικές εξελίξεις ή αλλαγές στο επιχειρησιακό τους μοντέλο.

Τρίτη σημαντική κατηγορία καλών πρακτικών αφορά τη διαχείριση των σχέσεων με προμηθευτές. Η συμβατική θωράκιση θεωρείται κρίσιμη, καθώς μέσω αυτής καθορίζονται ρητά οι απαιτήσεις ασφάλειας. Οι συμβάσεις θα πρέπει να περιλαμβάνουν ρήτρες προστασίας πληροφοριών, υποχρεώσεις γνωστοποίησης περιστατικών, δικαίωμα

ελέγχου (right to audit), καθώς και ρυθμίσεις για τη διαχείριση υπο-προμηθευτών. Παράλληλα, απαιτείται διαδικασία παρακολούθησης της απόδοσης των προμηθευτών, ώστε να διασφαλίζεται ότι οι συμφωνημένες απαιτήσεις ασφάλειας τηρούνται στην πράξη. Η διαχείριση αλλαγών – για παράδειγμα σε τεχνολογίες ή εργαλεία που χρησιμοποιούνται – πρέπει επίσης να αποτελεί μέρος της οργανωμένης εποπτείας της σχέσης.

Ιδιαίτερη έμφαση αποδίδεται στη διαχείριση ευπαθειών (vulnerability handling), η οποία αποτελεί κρίσιμο παράγοντα περιορισμού του κινδύνου διάχυσης απειλών μέσω της εφοδιαστικής αλυσίδας. Οι οργανισμοί οφείλουν να διατηρούν επικαιροποιημένο κατάλογο περιουσιακών στοιχείων, να παρακολουθούν ανακοινώσεις ευπαθειών και να εφαρμόζουν διαδικασίες διαχείρισης διορθωτικών ενημερώσεων (patch management) βάσει αξιολόγησης κινδύνου. Οι ενημερώσεις λογισμικού (patches) θα πρέπει να προέρχονται από αξιόπιστες πηγές, να ελέγχεται η ακεραιότητά τους και να δοκιμάζονται κατάλληλα πριν από την εγκατάστασή τους σε παραγωγικά συστήματα. Σε περιπτώσεις όπου δεν είναι άμεσα διαθέσιμη η ενημέρωση, θα πρέπει να εξετάζονται εναλλακτικά μέτρα μετριασμού του κινδύνου. Η χρήση εργαλείων όπως το Software Bill of Materials (SBOM) ενισχύει τη διαφάνεια σχετικά με τα επιμέρους στοιχεία ενός προϊόντος και διευκολύνει την έγκαιρη αναγνώριση επηρεαζόμενων συστημάτων. Τέλος, ο ENISA αναδεικνύει τη σημασία της ποιότητας προϊόντων και πρακτικών των προμηθευτών. Η ασφάλεια πρέπει να ενσωματώνεται ήδη από το στάδιο του σχεδιασμού και της ανάπτυξης προϊόντων (secure development lifecycle), με υιοθέτηση αναγνωρισμένων προτύπων και διαδικασιών διασφάλισης ποιότητας. Οι οργανισμοί-πελάτες οφείλουν να τηρούν διαφανείς διαδικασίες ως προς τις πρακτικές κυβερνοασφάλειας των προμηθευτών τους και να εφαρμόζουν πολιτικές αποδοχής και ελέγχου των παραδοτέων προϊόντων και υπηρεσιών. Η ποιότητα δεν είναι στατική ιδιότητα, αλλά αποτέλεσμα συνεχούς βελτίωσης και ελέγχου.

Συνολικά, σύμφωνα με τον ENISA, η ασφάλεια της εφοδιαστικής αλυσίδας προϋποθέτει συνδυασμό στρατηγικής διακυβέρνησης, συστηματικής διαχείρισης κινδύνων, συμβατικής ενσωμάτωσης απαιτήσεων ασφάλειας, ώριμης διαχείρισης ευπαθειών και ελέγχου της ποιότητας προϊόντων και υπηρεσιών. Η υιοθέτηση των πρακτικών αυτών ενισχύει τη διαφάνεια, τη λογοδοσία και την ανθεκτικότητα των

οργανισμών απέναντι σε συστημικούς κυβερνοκινδύνους που αναδύονται μέσα από το σύγχρονο, διασυνδεδεμένο ψηφιακό οικοσύστημα.

8.6 Μεθοδολογικό πλαίσιο μελέτης και εφαρμογής της διαχείρισης κινδύνων τρίτων μερών (Third Party Risk Management)

Η διαχείριση κινδύνων τρίτων μερών (Third Party Risk Management – TPRM) δεν μπορεί να περιορίζεται σε αποσπασματικές αξιολογήσεις προμηθευτών ή σε τυπικές συμβατικές ρήτρες. Αντιθέτως, απαιτεί ένα συνεκτικό και πολυεπίπεδο μεθοδολογικό πλαίσιο, το οποίο να συνδυάζει τεχνική χαρτογράφηση εξαρτήσεων, συστηματική αξιολόγηση κινδύνου, νομική θωράκιση και συνεχή εποπτεία. Στο πλαίσιο της ασφάλειας εφοδιαστικής αλυσίδας, η μεθοδολογική προσέγγιση οφείλει να είναι δυναμική, τεκμηριωμένη και πλήρως ενσωματωμένη στο σύστημα διακυβέρνησης του οργανισμού.

Αφετηρία της μεθοδολογίας αποτελεί η χαρτογράφηση της εφοδιαστικής αλυσίδας. Η διαδικασία αυτή περιλαμβάνει την πλήρη καταγραφή όλων των άμεσων προμηθευτών και παρόχων υπηρεσιών Τεχνολογιών Πληροφορικής και Επικοινωνιών, καθώς και των κρίσιμων προϊόντων και υπηρεσιών που παρέχουν.

Η χαρτογράφηση δεν περιορίζεται στους άμεσους συμβατικούς συνεργάτες (Tier 1), αλλά επεκτείνεται, στο μέτρο του εφικτού, στους προμηθευτές δεύτερου και τρίτου επιπέδου (Tier 2 και Tier 3), ιδίως όταν οι τελευταίοι επηρεάζουν κρίσιμες λειτουργίες. Η πολυεπίπεδη αυτή προσέγγιση επιτρέπει την κατανόηση των έμμεσων εξαρτήσεων και των πιθανών αλυσιδωτών επιπτώσεων σε περίπτωση αστοχίας ή παραβίασης.

Σημαντικό εργαλείο της χαρτογράφησης αποτελεί το Software Bill of Materials (SBOM), το οποίο παρέχει αναλυτική αποτύπωση των επιμέρους στοιχείων λογισμικού που περιλαμβάνονται σε ένα προϊόν ή σύστημα. Μέσω του SBOM ενισχύεται η διαφάνεια ως προς τις βιβλιοθήκες, τα modules και τις εξαρτήσεις τρίτων, διευκολύνοντας την έγκαιρη αναγνώριση ευπαθειών και τον στοχευμένο περιορισμό κινδύνων. Η ύπαρξη επικαιροποιημένου SBOM συμβάλλει ουσιαστικά στην τεχνική τεκμηρίωση του κινδύνου και στη διαμόρφωση τεκμηριωμένων αποφάσεων.

Σε δεύτερο στάδιο, η χαρτογράφηση μετατρέπεται σε αξιολόγηση μέσω της εφαρμογής μήτρας ταξινόμησης κινδύνου (risk classification matrix). Η μεθοδολογία

βασίζεται στη συσχέτιση της πιθανότητας (likelihood) επέλευσης ενός περιστατικού με τη σοβαρότητα των επιπτώσεων (impact). Η ανάλυση αυτή οδηγεί σε κατηγοριοποίηση των προμηθευτών βάσει κρισιμότητας, λαμβάνοντας υπόψη παράγοντες όπως η πρόσβαση σε κρίσιμα συστήματα, η επεξεργασία ευαίσθητων δεδομένων και ο ρόλος τους στην επιχειρησιακή συνέχεια. Η αποτύπωση της κρισιμότητας μπορεί να πραγματοποιείται μέσω συστήματος βαθμολόγησης (criticality scoring), το οποίο επιτρέπει τη συγκριτική αξιολόγηση και την ιεράρχηση προτεραιοτήτων. Επιπλέον, σε τομείς ιδιαίτερης σημασίας, η αξιολόγηση δύναται να ενσωματώνει τομεακή προτεραιοποίηση (sectoral prioritization), ώστε να λαμβάνονται υπόψη ειδικά ρυθμιστικά και επιχειρησιακά χαρακτηριστικά.

Η τεχνική και ποσοτική αξιολόγηση κινδύνου συμπληρώνεται από τον νομικό έλεγχο των συμβατικών σχέσεων. Ο νομικός έλεγχος δεν περιορίζεται στη διατύπωση γενικών ρητρών ασφάλειας, αλλά εξετάζει τη σαφήνεια, την εκτελεστότητα και την επάρκεια των προβλέψεων. Κρίσιμες θεωρούνται οι ρήτρες που καθορίζουν ελάχιστες απαιτήσεις κυβερνοασφάλειας, η πρόβλεψη δικαιώματος ελέγχου (audit rights), οι υποχρεώσεις άμεσης γνωστοποίησης περιστατικών (incident notification clauses), καθώς και ρυθμίσεις σχετικά με τη γεωγραφική τοποθεσία αποθήκευσης και επεξεργασίας δεδομένων (data localization). Η ενσωμάτωση των όρων αυτών δημιουργεί σαφές πλαίσιο ευθυνών και ενισχύει τη δυνατότητα επιβολής διορθωτικών μέτρων.

Η μεθοδολογία ολοκληρώνεται με την εφαρμογή διαδικασιών δέουσας επιμέλειας (due diligence) και συνεχούς παρακολούθησης. Πριν από τη σύναψη σύμβασης, διενεργείται προ-συμβατική αξιολόγηση του προμηθευτή, η οποία μπορεί να περιλαμβάνει ερωτηματολόγια ασφάλειας (security questionnaires), αξιολόγηση πιστοποιήσεων, καθώς και εξέταση ιστορικού περιστατικών. Σε περιπτώσεις υψηλής κρισιμότητας, είναι σκόπιμη η διενέργεια επιτόπιων ελέγχων (on-site audits) ή ανεξάρτητων αξιολογήσεων. Ωστόσο, η δέουσα επιμέλεια δεν εξαντλείται στο στάδιο επιλογής. Η συνεχής παρακολούθηση της κυβερνοασφαλούς στάσης (continuous cyber posture monitoring) του προμηθευτή, μέσω τεχνικών εργαλείων και περιοδικών επαναξιολογήσεων, αποτελεί αναγκαία προϋπόθεση για τη διατήρηση αποδεκτού επιπέδου κινδύνου.

Συνολικά, το μεθοδολογικό πλαίσιο TPRM συνιστά έναν κύκλο διαρκούς βελτίωσης, όπου η χαρτογράφηση, η αξιολόγηση, η νομική θωράκιση και η εποπτεία λειτουργούν αλληλοσυμπληρωματικά. Η αποτελεσματική εφαρμογή του πλαισίου αυτού ενισχύει τη διαφάνεια, τη λογοδοσία και την ανθεκτικότητα του οργανισμού απέναντι σε συστημικούς κινδύνους που αναδύονται από τις εξαρτήσεις του στο σύγχρονο ψηφιακό οικοσύστημα.

Μεθοδολογικό πλαίσιο μελέτης και εφαρμογής της διαχείρισης κινδύνων τρίτων μερών (Third Party Risk Management)

8.7 Ανάγκη εκπόνησης εξειδικευμένης πολιτικής ασφάλειας εφοδιαστικής αλυσίδας και διαχείρισης κινδύνων τρίτων μερών

Στο πλαίσιο της διαχείρισης κινδύνων στην εφοδιαστική αλυσίδα, ανακύπτει σαφής ανάγκη για την κατάρτιση και εκπόνηση Πολιτικής Διαχείρισης Προμηθευτών, η οποία θα θεμελιώνει ένα βασικό οργανωτικό και συμβατικό πλαίσιο ελέγχου των σχέσεων του οργανισμού με τρίτα μέρη. Η πολιτική αυτή οφείλει να ρυθμίζει κατ' ελάχιστον ζητήματα όπως η τήρηση επικαιροποιημένου μητρώου συνεργατών, η ενσωμάτωση ρητρών

ασφάλειας πληροφοριών στις συμβάσεις, η διαχείριση φυσικών και λογικών προσβάσεων, καθώς και οι διαδικασίες αναφοράς και διαχείρισης περιστατικών ασφάλειας. Με τον τρόπο αυτό, δημιουργείται μια θεσμική βάση διαφάνειας, λογοδοσίας και ελέγχου στις σχέσεις με προμηθευτές και εξωτερικούς συνεργάτες.

Ωστόσο, η σύγχρονη κανονιστική πραγματικότητα και η αυξημένη πολυπλοκότητα των ψηφιακών εξαρτήσεων καθιστούν σαφές ότι η απλή ύπαρξη μιας γενικής πολιτικής διαχείρισης προμηθευτών δεν επαρκεί. Οι οργανισμοί λειτουργούν πλέον εντός ενός διασυνδεδεμένου και πολυεπίπεδου τεχνολογικού οικοσυστήματος, στο οποίο συμμετέχουν πάροχοι λογισμικού, υπηρεσιών νεφοϋπολογιστικής, διαχειριζόμενων υπηρεσιών, καθώς και υπο-προμηθευτές δεύτερου και τρίτου επιπέδου. Οι εξαρτήσεις αυτές είναι συχνά μη ορατές σε πλήρη έκταση, ενώ η παραβίαση ή αστοχία ενός κρίσιμου κρίκου της αλυσίδας μπορεί να προκαλέσει αλυσιδωτές επιπτώσεις στην επιχειρησιακή συνέχεια, στην ασφάλεια δεδομένων και στη φήμη του οργανισμού.

Η ανάγκη, επομένως, για εκπόνηση διακριτής και εξειδικευμένης Πολιτικής Ασφάλειας Εφοδιαστικής Αλυσίδας και Διαχείρισης Κινδύνων Τρίτων Μερών απορρέει από τη διαπίστωση ότι η διαχείριση προμηθευτών δεν αποτελεί απλώς διοικητική ή συμβατική διαδικασία, αλλά κρίσιμο πυλώνα του συνολικού πλαισίου διακυβέρνησης κινδύνων. Η νέα αυτή πολιτική πρέπει να λειτουργεί συμπληρωματικά προς την υφιστάμενη Πολιτική Διαχείρισης Προμηθευτών, εστιάζοντας ρητώς στη συστηματική αναγνώριση, αξιολόγηση και παρακολούθηση των κινδύνων που απορρέουν από την εφοδιαστική αλυσίδα.

Ειδικότερα, η εξειδικευμένη πολιτική οφείλει να ενσωματώνει σαφές μεθοδολογικό πλαίσιο χαρτογράφησης και κατηγοριοποίησης των προμηθευτών, με βάση την κρισιμότητα των παρεχόμενων υπηρεσιών, την πρόσβαση σε κρίσιμα συστήματα ή δεδομένα και τον δυνητικό αντίκτυπο σε περίπτωση διακοπής ή παραβίασης. Η αξιολόγηση αυτή πρέπει να στηρίζεται σε τεκμηριωμένη ανάλυση πιθανότητας και αντίκτυπου, να οδηγεί σε κατηγοριοποίηση κινδύνου και να επαναλαμβάνεται σε τακτά χρονικά διαστήματα ή σε περίπτωση ουσιωδών αλλαγών στη σχέση με τον προμηθευτή.

Παράλληλα, η πολιτική πρέπει να εξειδικεύει τις ελάχιστες απαιτήσεις ασφάλειας που επιβάλλονται στους προμηθευτές, καθορίζοντας υποχρεωτικά συμβατικά στοιχεία, όπως ρήτρες ασφάλειας πληροφοριών, δικαιώματα ελέγχου και επιθεώρησης,

υποχρεώσεις έγκαιρης γνωστοποίησης περιστατικών, ρυθμίσεις για τη διαχείριση υπο-προμηθευτών και πρόνοιες σχετικά με τη γεωγραφική τοποθεσία αποθήκευσης ή επεξεργασίας δεδομένων. Ιδιαίτερη έμφαση πρέπει να δίδεται στη διαχείριση κρίσιμων προμηθευτών, καθώς και στη διασφάλιση ύπαρξης σαφούς στρατηγικής αποχώρησης (exit strategy), ώστε να καθίσταται εφικτή η ομαλή μετάβαση σε εναλλακτικό πάροχο σε περίπτωση διακοπής συνεργασίας.

Επιπλέον, η πολιτική οφείλει να προβλέπει διαδικασίες δέουσας επιμέλειας πριν από τη σύναψη συμβάσεων, όπως αξιολόγηση πιστοποιήσεων, ερωτηματολόγια ασφάλειας και, όπου απαιτείται, επιτόπιους ελέγχους. Η διαχείριση κινδύνου, ωστόσο, δεν πρέπει να περιορίζεται στο στάδιο επιλογής· απαιτείται συνεχής παρακολούθηση του κυβερνοασφαλούς προφίλ των συνεργατών και επαναξιολόγηση των κινδύνων σε όλη τη διάρκεια της συνεργασίας.

Τέλος, η εξειδικευμένη αυτή πολιτική πρέπει να εντάσσεται οργανικά στο ευρύτερο πλαίσιο εταιρικής διακυβέρνησης. Πρέπει να καθορίζονται σαφώς οι ρόλοι και οι ευθύνες των εμπλεκόμενων λειτουργιών, να προβλέπονται μηχανισμοί αναφοράς προς τη διοίκηση και να θεσπίζεται τακτική αναθεώρηση της πολιτικής, ώστε να ανταποκρίνεται στις μεταβαλλόμενες απειλές και κανονιστικές απαιτήσεις. Με τον τρόπο αυτό, η διαχείριση κινδύνων τρίτων μερών μετατρέπεται από επιμέρους λειτουργική διαδικασία σε στρατηγικό εργαλείο ενίσχυσης της οργανωτικής ανθεκτικότητας και της κανονιστικής συμμόρφωσης.

9. ΣΥΜΠΕΡΑΣΜΑΤΑ

Η παρούσα διπλωματική εργασία εξέτασε το κανονιστικό πλαίσιο της Ευρωπαϊκής Οδηγίας (ΕΕ) 2022/2555 (NIS2) και την ενσωμάτωσή της στο ελληνικό δίκαιο μέσω του Νόμου 5160/2024, με έμφαση στην κυβερνοασφάλεια και στη διαμόρφωση ενός πρακτικού πλαισίου ελέγχου συμμόρφωσης για επιχειρήσεις και οργανισμούς. Σε ένα περιβάλλον ραγδαίου ψηφιακού μετασχηματισμού και αυξανόμενων κυβερνοαπειλών, η NIS2 σηματοδοτεί μια ουσιαστική μετατόπιση της ευρωπαϊκής προσέγγισης, από την αποσπασματική τεχνική προστασία προς ένα ολοκληρωμένο μοντέλο διακυβέρνησης

της κυβερνοασφάλειας, βασισμένο στη διαχείριση κινδύνων, στη λογοδοσία και στη θεσμική ευθύνη.

Ένα από τα βασικά συμπεράσματα της εργασίας είναι ότι η κυβερνοασφάλεια, στο πλαίσιο της NIS2, δεν μπορεί πλέον να αντιμετωπίζεται ως αποκλειστική αρμοδιότητα των τεχνικών τμημάτων πληροφορικής. Αντιθέτως, αναδεικνύεται σε στρατηγικό ζήτημα διοίκησης και συμμόρφωσης, το οποίο απαιτεί ενεργό συμμετοχή του ανώτατου οργάνου διοίκησης των οργανισμών. Η σύνδεση της κυβερνοασφάλειας με τη διακυβέρνηση και τη νομική ευθύνη αντικατοπτρίζει την πραγματικότητα ότι τα περιστατικά κυβερνοασφάλειας δύνανται να επιφέρουν σοβαρές επιχειρησιακές, οικονομικές, κοινωνικές και θεσμικές επιπτώσεις, υπερβαίνοντας τα όρια μιας απλής τεχνικής δυσλειτουργίας.

Η ανάλυση των μορφών και τύπων κυβερνοεπιθέσεων κατέδειξε ότι οι σύγχρονες απειλές χαρακτηρίζονται από αυξημένη πολυπλοκότητα και συχνά εκμεταλλεύονται όχι μόνο τεχνικές ευπάθειες, αλλά και οργανωτικές αδυναμίες και ανθρώπινους παράγοντες. Επιθέσεις κοινωνικής μηχανικής, εκστρατείες phishing, περιστατικά ransomware και επιθέσεις στην εφοδιαστική αλυσίδα αναδεικνύουν την ανάγκη για μια πολυεπίπεδη προσέγγιση ασφάλειας, η οποία συνδυάζει τεχνικά μέτρα, οργανωτικές πολιτικές, εκπαίδευση προσωπικού και συνεχή αξιολόγηση κινδύνων. Το εύρημα αυτό επιβεβαιώνει τη φιλοσοφία της NIS2, η οποία απομακρύνεται από στενά τεχνικές λύσεις και προκρίνει μια συνολική διαχείριση της κυβερνοασφάλειας.

Ιδιαίτερη σημασία αναδείχθηκε στον ρόλο των οργανωτικών προτύπων ασφάλειας πληροφοριών και ειδικότερα στη συμβολή διεθνών προτύπων, όπως το ISO/IEC 27001, στην υποστήριξη της συμμόρφωσης με τη NIS2. Αν και η Οδηγία δεν επιβάλλει υποχρεωτική πιστοποίηση, η υιοθέτηση τέτοιων πλαισίων παρέχει στις επιχειρήσεις – και ιδίως στις μικρομεσαίες – ένα δομημένο και πρακτικό εργαλείο για την εφαρμογή αναλογικών μέτρων ασφάλειας, τη σαφή κατανομή ρόλων και την καλλιέργεια κουλτούρας ασφάλειας. Η προσέγγιση αυτή διευκολύνει τόσο την κανονιστική συμμόρφωση όσο και την ενίσχυση της συνολικής ανθεκτικότητας των οργανισμών.

Η εξέταση του ελληνικού θεσμικού πλαισίου ανέδειξε ότι ο Ν. 5160/2024 αποτελεί ένα σημαντικό βήμα προς την εδραίωση ενός σύγχρονου και συνεκτικού συστήματος

διακυβέρνησης της κυβερνοασφάλειας στη χώρα. Μέσω της σαφούς οριοθέτησης των αρμόδιων αρχών, της καθιέρωσης υποχρεώσεων αναφοράς περιστατικών και της πρόβλεψης μηχανισμών εποπτείας και κυρώσεων, ο νόμος δημιουργεί τις προϋποθέσεις για αποτελεσματική εφαρμογή της NIS2 σε εθνικό επίπεδο. Παράλληλα, η λειτουργία της Εθνικής Αρχής Κυβερνοασφάλειας και των εθνικών CSIRT ενισχύει τον συντονισμό, τη συνεργασία και την ανταλλαγή πληροφοριών, τόσο εντός της χώρας όσο και σε ευρωπαϊκό επίπεδο.

Κρίσιμη αναδείχθηκε και η θεσμοθέτηση ρόλων εντός των οργανισμών, με χαρακτηριστικό παράδειγμα τον Υπεύθυνο Ασφάλειας Συστημάτων Πληροφορικής και Επικοινωνιών (Υ.Α.Σ.Π.Ε.) ή CISO. Ο ρόλος αυτός λειτουργεί ως συνδετικός κρίκος μεταξύ της διοίκησης, των τεχνικών ομάδων και των αρμόδιων αρχών, διασφαλίζοντας την υλοποίηση, παρακολούθηση και συνεχή βελτίωση των μέτρων κυβερνοασφάλειας. Η αποτελεσματικότητα της συμμόρφωσης με τη NIS2 εξαρτάται σε μεγάλο βαθμό από τη σαφή κατανομή αρμοδιοτήτων και τη λειτουργική ενσωμάτωση του ρόλου αυτού στη διοικητική δομή του οργανισμού.

Η ανάλυση των τεχνικών και οργανωτικών μέτρων ασφάλειας κατέδειξε ότι η συμμόρφωση με τη NIS2 δεν επιτυγχάνεται μέσω μεμονωμένων ελέγχων, αλλά μέσω ενός ολοκληρωμένου συστήματος πολιτικών, διαδικασιών και τεχνικών μέτρων. Ο έλεγχος πρόσβασης, η ασφαλής παραμετροποίηση συστημάτων, η κρυπτογράφηση, η διαχείριση περιστατικών, η ασφάλεια της εφοδιαστικής αλυσίδας και η φυσική ασφάλεια συνιστούν αλληλένδετα στοιχεία ενός ενιαίου πλαισίου προστασίας. Η αρχή της αναλογικότητας που ενσωματώνει η NIS2 επιτρέπει την προσαρμογή των μέτρων αυτών στο εκάστοτε προφίλ κινδύνου, καθιστώντας το πλαίσιο εφαρμόσιμο σε οργανισμούς διαφορετικού μεγέθους και πολυπλοκότητας.

Ιδιαίτερη έμφαση δόθηκε στις υποχρεώσεις αναφοράς περιστατικών κυβερνοασφάλειας, οι οποίες συνιστούν θεμελιώδες στοιχείο της NIS2. Η έγκαιρη κοινοποίηση περιστατικών, η τήρηση συγκεκριμένων χρονοδιαγραμμάτων και η υποβολή τελικών εκθέσεων συμβάλλουν στη διαφάνεια, στη λογοδοσία και στη συλλογική κατανόηση του τοπίου των απειλών. Η αναφορά περιστατικών δεν θα πρέπει να αντιμετωπίζεται αποκλειστικά ως κανονιστική επιβάρυνση, αλλά ως εργαλείο

μάθησης και βελτίωσης, το οποίο ενισχύει τη συνολική ανθεκτικότητα του ψηφιακού οικοσυστήματος.

Τέλος, η ένταξη της επιχειρησιακής συνέχειας και της διαχείρισης κρίσεων στο πλαίσιο της κυβερνοασφάλειας υπογραμμίζει την παραδοχή ότι τα περιστατικά κυβερνοασφάλειας δεν μπορούν να αποκλειστούν πλήρως. Η ικανότητα ενός οργανισμού να ανιχνεύει, να αποκρίνεται και να ανακάμπτει αποτελεσματικά από τέτοια περιστατικά αποτελεί κρίσιμο δείκτη ψηφιακής ανθεκτικότητας. Η NIS2, σε συνδυασμό με τον Ν. 5160/2024, θέτει τις βάσεις για μια ώριμη και ρεαλιστική προσέγγιση, η οποία ενσωματώνει την πρόληψη, την ετοιμότητα και την αποκατάσταση ως αλληλένδετα στάδια ενός ενιαίου κύκλου διαχείρισης κινδύνων.

Συνολικά, η παρούσα εργασία καταδεικνύει ότι η Οδηγία NIS2 και το εθνικό εφαρμοστικό πλαίσιο συνιστούν ένα σύγχρονο και δυναμικό σύστημα διακυβέρνησης της κυβερνοασφάλειας, το οποίο μπορεί να λειτουργήσει αποτελεσματικά μόνο εφόσον υιοθετηθεί ουσιαστικά από τις υπόχρεες οντότητες. Η συμμόρφωση δεν θα πρέπει να περιορίζεται σε τυπική εκπλήρωση υποχρεώσεων, αλλά να αξιοποιείται ως ευκαιρία για την βελτίωση της οργανωτικής ωριμότητας, την ενίσχυση της ανθεκτικότητας και την οικοδόμηση εμπιστοσύνης σε ένα ολοένα και πιο απαιτητικό ψηφιακό περιβάλλον.

ΒΙΒΛΙΟΓΡΑΦΙΚΕΣ ΠΗΓΕΣ ΚΑΙ ΑΝΑΦΟΡΕΣ

Νομικά Πλαίσια & Κανονιστικά Κείμενα

European Union (2022) *Directive (EU) 2022/2555 of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union*, Official Journal of the European Union, L 333.

Hellenic Republic (2024) *Law 5160/2024 on Cybersecurity*, Government Gazette.

European Union (2016) *Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation)*, Official Journal of the European Union, L 119.

European Union Agency for Cybersecurity (ENISA) (2020) *NIS2 Directive: Analysis and Implementation Guidance*, ENISA.

Ministry of Digital Governance (Greece) (2025) *Ministerial Decision 1689/2025 – National Framework of Cybersecurity Requirements for Essential and Important Entities*, Government Gazette.

Διεθνή Πρότυπα & Τεχνικά Πλαίσια

International Organization for Standardization (2013) *ISO/IEC 27001:2013 – Information technology – Security techniques – Information security management systems – Requirements*, ISO.

International Organization for Standardization (2013) *ISO/IEC 27002:2013 – Information technology – Security techniques – Code of practice for information security controls*, ISO.

National Institute of Standards and Technology (2018) *Framework for Improving Critical Infrastructure Cybersecurity*, NIST, Version 1.1.

European Union Agency for Cybersecurity (2023). *Good Practices for Supply Chain Cybersecurity*. June 2023. (Κατευθυντήριο κείμενο που παρουσιάζει ολοκληρωμένο πλαίσιο καλών πρακτικών για τη διαχείριση κινδύνων στην εφοδιαστική αλυσίδα ICT/OT, με έμφαση στη διακυβέρνηση, στη διαχείριση ευπαθειών και στη συμβατική θωράκιση)

European Union Agency for Cybersecurity (2021). *Threat Landscape for Supply Chain Attacks.* (Ανάλυση της απειλητικής δυναμικής των επιθέσεων εφοδιαστικής αλυσίδας, με στατιστικά δεδομένα, τυπολογία επιθέσεων και συστημικές επιπτώσεις)

National Institute of Standards and Technology (2022). *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations* (NIST SP 800-161 Rev.1). (Πρότυπο αναφοράς για την ενσωμάτωση της διαχείρισης κινδύνων εφοδιαστικής αλυσίδας στο Enterprise Risk Management)

International Organization for Standardization / International Electrotechnical Commission (2022). ISO/IEC 27036 – *Information security for supplier relationships.* (Διεθνές πρότυπο που καθορίζει απαιτήσεις και κατευθυντήριες γραμμές για την ασφάλεια στις σχέσεις με προμηθευτές)

Επιστημονικά Άρθρα & Papers

Bada, M. and Nurse, J.R.C. (2019) 'Developing cybersecurity education and awareness programmes for small-to-medium enterprises (SMEs)', *Information & Computer Security*, 27(3), pp. 393–410.

Böhme, R. (2016) 'Cyber insurance as a risk management strategy', *Annual Review of Financial Economics*, 8, pp. 677–702.

European Union Agency for Cybersecurity (ENISA) (2021) 'Threat Landscape Report 2021', ENISA.

Farahmand, F. and Martin, A. (2020) 'A survey on cyber threats and defence mechanisms for small and medium enterprises (SMEs)', *Journal of Cyber Security and Mobility*, 9(2), pp. 205–230.

Kostopoulos, G.K., Bampis, L. and Marinos, L. (2021) 'A risk management framework for GDPR and NIS2 compliance in modern digital infrastructures', *Journal of Information Security and Applications*, 59, 102910.

Leitch, S. and Warren, M.J. (2021) 'Cybersecurity governance in practice: A multiple case study of cybersecurity policy implementation in organizations', *Computers & Security*, 109, 102398.

Olya, H.G.T. and Khatibi, A. (2018) 'Cybersecurity risk management: A review of standards, frameworks and literature', *International Journal of Cybersecurity Intelligence & Cybercrime*, 1(2), pp. 1–12.

Papathanasiou, A., Georgios L., Vasiliki L., and Glavas, A. "Business Email Compromise (BEC) Attacks: Threats, Vulnerabilities and Countermeasures—A Perspective

on the Greek Landscape." *Journal of Cybersecurity and Privacy* 3, no. 3 (2023): 610–637. https://doi.org/10.3390/jcp3030029

Romanosky, S. (2016) 'Examining the costs and causes of cyber incidents', *Journal of Cybersecurity*, 2(2), pp. 121–135.

Shaw, P. and Caelli, W. (2021) 'Incident response and management: best practices and lessons learned', *Information Systems Frontiers*, 23, pp. 1037–1054.

Sommer, P. (2017) 'What makes cyber risk different than other operational risks?', *Risk Management and Insurance Review*, 20(1), pp. 69–93.

Βιβλία & Επιστημονικές Εκδόσεις

Anderson, R. (2020) *Security Engineering: A Guide to Building Dependable Distributed Systems*, 3rd edn, Wiley.

Bishop, M. (2021) *Introduction to Computer Security*, 2nd edn, Addison-Wesley.

Mansfield-Devine, S. (2019) *The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations*, Routledge.

Pfleeger, C.P. and Pfleeger, S.L. (2015) *Security in Computing*, 5th edn, Pearson.

Papathanasiou, A., Cybersecurity, Disigma Publications, 2025.

Hellenic Federation of Enterprises (SEV), NIS2 European Directive: From Compliance to Resilience – A Practical Guide for Businesses, SEV Business Support Center (SEV Stegi), 2025.

Stallings, W. (2018) *Network Security Essentials: Applications and Standards*, 6th edn, Pearson.

Reports & Τεχνικές Εκθέσεις

ENISA (2023) *Annual Incident Reports and Cybersecurity Trends*, European Union Agency for Cybersecurity.

Gartner (2021) *Cybersecurity Risk Management Best Practices for Compliance*, Gartner Research.

ISACA (2022) *COBIT for Cybersecurity*, ISACA.

Verizon (2023) *Data Breach Investigations Report*, Verizon.

World Economic Forum (2020) *Global Risks Report 2020*, World Economic Forum.

Ιστοσελίδες

https://cyber.gov.gr/

https://www.dpa.gr/

https://www.nis.gr/el/national-cert/

https://adae.gov.gr/

https://dsa.cy/

https://dsa.cy/images/pdf-upload/nis2-guide.pdf

https://www.sev.org.gr/